

**UNITED STATES DISTRICT COURT  
SOUTHERN DISTRICT OF NEW YORK**

IN RE BLOCK, INC. SECURITIES  
LITIGATION

No. 1:22-cv-08636 (MMG)

CLASS ACTION

DEMAND FOR JURY TRIAL

---

**CONSOLIDATED COMPLAINT  
FOR VIOLATIONS OF THE FEDERAL SECURITIES LAWS**

## TABLE OF CONTENTS

	<u>Page</u>
I. NATURE OF ACTION .....	1
II. JURISDICTION AND VENUE .....	2
III. PARTIES .....	3
IV. SUBSTANTIVE ALLEGATIONS APPLICABLE TO ALL CLAIMS .....	5
A. Block’s Business Depends Upon Obtaining and Safeguarding the Personally Identifiable Information of Its Customers.....	5
B. Defendants Acknowledge and Identify Substantial Potential Cybersecurity Risks .....	6
C. Block Violated Accepted Industry Cybersecurity Standards, Resulting in a Massive Undisclosed Data Breach .....	9
D. The Aftermath and Block’s Reaction to the Data Breach.....	14
E. Materially False or Misleading Statements Made to Afterpay Shareholders.....	15
1. Statements Regarding Block’s Internal Controls to Facilitate the Merger .....	15
2. Defendant Dorsey’s Involvement in the Afterpay Merger .....	20
V. CLASS ACTION ALLEGATIONS .....	29
FIRST CAUSE OF ACTION: (Brought by OIP, Only, for Violation of § 12(a)(2) of the Securities Act on Behalf of the Securities Act Class, Against Block and Dorsey).....	31
SECOND CAUSE OF ACTION: (Brought by OIP, Only, for Violations of § 15(a) of the Securities Act on Behalf of the Securities Act Class, Against Dorsey and McKelvey).....	34
VI. ADDITIONAL ALLEGATIONS FOR EXCHANGE ACT CLAIMS BY ALL EXCHANGE ACT CLASS MEMBERS.....	35
A. Additional Exchange Act Materially False or Misleading Statements Issued During the Class Period .....	35
B. Scierter .....	45

1.	Block and the Individual Defendants Were Long Aware of Red Flags Demonstrating Block’s Derelict Data Security Practices .....	45
2.	Defendants Are Presumed to Have Had Near Contemporaneous Knowledge of Security Breaches.....	47
3.	Motive .....	50
4.	Secrecy and Lack of Cooperation with Regulators.....	50
C.	Loss Causation.....	52
D.	Presumption of Reliance .....	54
E.	Inapplicability of Statutory Safe Harbor.....	56
THIRD CAUSE OF ACTION: (Brought by Sotiropoulos and Sawyer, Only, for Violation of § 10(b) of the Exchange Act and Rule 10b-5(a), (b) and (c) Thereunder on Behalf of the Exchange Act Class, Against All Defendants) .....		56
FOURTH CAUSE OF ACTION: (Brought by Sotiropoulos and Sawyer, Only, Violation of § 20(a) of the Exchange Act on Behalf of the Exchange Act Class, Against All Individual Defendants) .....		59
PRAYER FOR RELIEF .....		59
DEMAND FOR JURY TRIAL .....		60

Lead Plaintiffs Fotios Sotiropoulos (“Sotiropoulos”) and Official Intelligence Pty. Ltd. (“OIP” or “Official Intelligence” and with Sotiropoulos the “Lead Plaintiffs”) and additional Plaintiff Kevin Sawyer (together with Lead Plaintiffs, “Plaintiffs”), by their undersigned attorneys, allege the following based upon personal knowledge as to Plaintiffs and their own acts, and upon information and belief as to other matters based on the investigation conducted by and through Plaintiffs’ attorneys, including reviewing U.S. Securities and Exchange Commission (“SEC”) filings of Block, Inc. f/k/a Square, Inc. (“Block” or the “Company”); Australian Securities and Investments Commission (“ASIC”) filings of Afterpay Limited (also referred to as “Afterpay”); court filings made In the Matter of Afterpay Limited [2021] (N.S.W.S. Ct.); press releases issued by Block; analyst reports; media reports; consultation with experts; a freedom of information act request; and other publicly available reports and information. Plaintiffs believe that substantial additional evidentiary support exists for the allegations set forth herein after a reasonable opportunity for discovery.

## **I. NATURE OF ACTION**

1. This action consolidates two distinct claims arising out of Defendants’ failure to disclose these material adverse facts: (a) fraud claims arising under §§ 10(b) and 20(a) of the Securities Exchange Act of 1934 (“Exchange Act”) and Rule 10b-5(a)-(c) promulgated thereunder (17 C.F.R. §240.10b-5) during the period February 26, 2020, to April 4, 2022 (the “Class Period”), with respect to which Sotiropoulos is serving as the Lead Plaintiff; and (b) a claim arising under §§12(a)(2) and 15 of the Securities Act of 1933 ( “Securities Act”) on behalf of former Afterpay shareholders who acquired unregistered Block, Inc. Class A common stock (the “Common Stock”) or corresponding SQ CHESS Depository Interests (“CDIs” and together with the Common Stock, “Block Shares” or “Block Securities”) pursuant to a “Scheme Booklet” through which Block

acquired Afterpay (the “Merger or “Transaction”) with respect to which Plaintiff OIP is serving as the Lead Plaintiff and which does not involve or require any allegations of either fraud or reliance.

2. Block, known as Square Inc. (also referred to herein as “Square”) before December 10, 2021, is a global technology company focusing on financial services, including Square, Cash App Investing LLC (“Cash App”), Spiral, and TIDAL. This case relates to Block’s failure to disclose the following material facts with respect to its operations: (a) Block lacked adequate security measures or controls sufficient to guard the confidentiality of its customers’ personally identifiable information (“PII” or “Private Information”) from known threats, including former employees being able to access and download PII; and (b) a former employee of Block accessed the Company’s networks on December 10, 2021, downloading the PII of approximately 8.2 million Cash App Investing users (the “Data Breach” or “First Data Breach”).

3. Block’s internal control weakness and the related breach of Block’s internal controls resulting in the release of users’ PII were disclosed through an April 4, 2022 filing Block made with the SEC, causing the price of Block Securities to decline from \$145.19 to \$123.22 and the price of the CDIs to decline from AUD 191.44 to AUD 164.48.

## **II. JURISDICTION AND VENUE**

4. This Court has original subject matter jurisdiction under 28 U.S.C. § 1331 because Plaintiffs assert claims arising under the Securities Act and Exchange Act, which are laws of the United States. The Company’s bylaws also designate the federal district courts of the United States as the exclusive forum for causes of action arising under the Securities Act.

5. Venue is proper in this District under § 22 of the Securities Act, 15 U.S.C. § 77v, and § 27 of the Exchange Act, 15 U.S.C. § 78aa, as well as under 28 U.S.C. § 1391, because: (a) the conduct at issue took place and had an effect in this District; (b) a substantial portion of the corporate transactions and wrongs complained of herein occurred here; (c) Defendants have

received substantial compensation and other transfers of money here by engaging in activities having an effect in this District; and (d) *Hart v. Block, Inc. et al.*, No. 3:23-cv-00455 (N.D. Cal. Jan. 31, 2023), having previously been transferred to this District pursuant to a Court-ordered stipulation entered into by Defendants Block, Jack Dorsey, and Amrita Ahuja.

### III. PARTIES

6. Lead Plaintiff Fotios Sotiropoulos purchased Block securities during the Class Period and was damaged as a result of the federal securities violations and misconduct alleged herein.

7. Lead Plaintiff Official Intelligence held 16,376 ordinary shares of Afterpay (“Afterpay Shares”) before the Transaction, and those Afterpay Shares were converted to 6,141 Block CDIs in connection with the Transaction closing and continued to hold Block CDIs at all relevant times.

8. Plaintiff Kevin Sawyer held 1,440 ordinary shares of Afterpay before the Transaction, and those ordinary shares were converted to 540 Block CDIs in connection with the Transaction closing and continued to hold Block CDIs at all relevant times.

9. Defendant Block is based in San Francisco, California, with its Class A common stock trading on the New York Stock Exchange (“NYSE”) under the symbol “SQ” and on the Australian Stock Exchange under the symbol “ASX” in the form of CDIs with each CDI representing a beneficial interest in one share of our Class A common stock. Block’s subsidiaries included Lanai (AU) 2 Pty Ltd (“Merger Sub”), which was created to facilitate the Transaction. Its Class A common stock trades under the ticker symbol “SQ” on the NYSE. In January 2022, Block acquired Afterpay by means of the Merger, and thereby distributed approximately 113 million Block Shares directly to former Afterpay shareholders in exchange for their Afterpay Limited stock.

10. Defendant Jack Dorsey (“Dorsey”) is Block’s co-founder and served as Block’s Chief Executive Officer (“CEO”) and President from July 2009 until April 2022 when he changed his title to “Block Head” and Chairperson of the Board. Additionally, Dorsey was a co-founder of Twitter and served as its CEO from July 2015 to November 29, 2021. As of March 31, 2022, the Company reported that Dorsey owned 48,844,566 Class B Block common shares, more than 43% of the Company’s voting power, effectively giving him voting control over Block. Defendant Dorsey reviewed and signed solicitation and other documents issued in connection with the Merger by which Lead Plaintiff OIP and other Afterpay shareholders were solicited to participate in the stock-for-stock exchange in connection with the Merger. Dorsey also wrote or signed a letter to holders of Afterpay shares that was included in the Scheme Booklet soliciting Afterpay’s shareholders’ approval of the Merger.

11. Defendant Amrita Ahuja (“Ahuja”) was at all relevant times the Chief Financial Officer for Block. Defendant Ahuja was directly and personally involved in negotiating the Merger on behalf of Block, and she executed, controlled, and implemented the terms and conditions by which the Merger, and consequent offers and sales of unregistered Block Shares, were effected. Defendant Ahuja signed the agreements and offering documents on behalf of Block by which Plaintiffs and other shareholders were solicited to participate in the stock-for-stock exchange in connection with the Merger. Through stock awards, bonuses, salary, and other incentives tied to the Merger, Defendant Ahuja realized millions of dollars in unjust enrichment.

12. Defendant Jim McKelvey is Block’s co-founder and a Board member. He owns over 12 million shares of Block’s common stock and is named herein as a control person of Block.

#### IV. SUBSTANTIVE ALLEGATIONS APPLICABLE TO ALL CLAIMS

##### A. Block's Business Depends Upon Obtaining and Safeguarding the Personally Identifiable Information of Its Customers

13. Block provides e-commerce services to small businesses. Block also offers a payment application called Cash App, initially designed to make peer-to-peer payments, *i.e.*, for consumers to transfer money to individuals and businesses, but which has since been configured for uses such as direct deposit payments, the purchasing of cryptocurrency, and other investments.

14. Cash App users must provide the Company with their personally identifiable information to open an account, which is collected and stored electronically by Block.

15. PII is a commodity that can be bought and sold just like oil and gas, farm products, and precious minerals. The market for PII is not a legal one but a thriving “black market” where sensitive financial information on a “CashApp verified account” has sold for hundreds of dollars (including during the period since the Data Breach of February 2021 to June 2022), a price driven by criminals’ ability to use the PII to target victims and steal their assets. Consumer victims of data breaches are more likely to become victims of identity fraud.<sup>1</sup> Indeed, studies confirm that the average direct financial loss for victims of identity theft in 2021 was \$1,100.<sup>2</sup>

16. The damage that can be caused by disclosure of PII makes potential Block customers sensitive about providing their PII. As a result, the Company seeks to reassure users with a related privacy notice that “explains how Square collects, uses and protects the personal

---

<sup>1</sup> 2014 LexisNexis True Cost of Fraud Study, LexisNexis (Aug. 2014), <https://risk.lexisnexis.com/-/media/files/corporations%20and%20non%20profits/research/true-cost-fraud-2014%20pdf.pdf>, at 6, 13.

<sup>2</sup> See Megan Leonhardt, *Consumers lost \$56 billion to identity fraud last year—here’s what to look out for*, CNBC (Mar. 23, 2021), <https://www.cnbc.com/2021/03/23/consumers-lost-56-billion-dollars-to-identity-fraud-last-year.html> (citing 2021 Identity Fraud Study by Javelin Strategy & Research).

information you provide to us where Square makes use of your personal data to provide you with the Services or for its own purposes.”<sup>3</sup>

17. The Company’s privacy notice also seeks to reassure Block’s customers by emphasizing, in a box designed to draw the reader’s attention, that: “*We do a lot to keep your data safe. While we think we have strong defenses in place, no one can ever guarantee that hackers won’t be able to break into our sites or steal your data while it is stored or flowing from you to us or vice versa.*”<sup>4</sup> Block’s privacy notice also stated that the Company takes “reasonable measures, including administrative, technical, and physical safeguards, to protect your information from loss, theft, and misuse, and unauthorized access, disclosure, alteration, and destruction.”<sup>5</sup>

18. Block’s ability to properly secure PII was also important to its customers. People and businesses almost universally dislike the disclosure of such information because, in addition to exposing them to potential fraud and harassment, the information is *private*. Therefore, any public perception that Block is not adequately protecting PII is harmful to its business.

## **B. Defendants Acknowledge and Identify Substantial Potential Cybersecurity Risks**

19. In public filings with the SEC, Block acknowledged the substantial risks that data loss or security breaches would pose to the Company. Thus, the risk factors section of the Company’s Annual Report on Form 10-K filed with the SEC on February 26, 2020 (the “2019 10-K”), stated that:

*If our privacy and security measures or those of third party developers and vendors are inadequate or are breached, and, as a*

---

<sup>3</sup> See *General Terms of Service*, Square (Apr. 26, 2021), <https://web.archive.org/web/20211104075402/https://squareup.com/us/en/legal/general/ua> (captured Nov. 4, 2021).

<sup>4</sup> See *Privacy Notice for Users Who Apply or Sign Up for a Square Account or Other Services*, Square (Jan. 1, 2020), <https://web.archive.org/web/20211104075354/https://squareup.com/us/en/legal/general/privacy> (captured Nov. 4, 2021).

<sup>5</sup> *Id.*

*result, there is improper disclosure of or someone obtains unauthorized access to or exfiltrates funds or sensitive information on our systems or our partners' systems, or if we suffer a ransomware or advanced persistent threat attack, or if any of the foregoing is reported or perceived to have occurred, our reputation and business could be damaged. If the sensitive information is lost or improperly accessed, misused, disclosed, destroyed, or altered or threatened to be improperly accessed, misused, disclosed, destroyed, or altered, we could incur significant financial losses and costs and liability associated with remediation and the implementation of additional security measures and be subject to litigation, regulatory scrutiny, and investigations.*

2019 10-K at 19.

20. The 2019 10-K also acknowledged that “electronic payment products and services, including ours, have been, and could continue to be in the future, specifically targeted and penetrated or disrupted by hackers,” *id.* at 20, posing a material risk to Block and its core operations because “*If we or our sellers or other customers are unable to anticipate or prevent these attacks, our sellers' or other customers' businesses may be harmed, our reputation could be damaged, and we could incur significant liability.*” *Id.* (emphasis added).

21. Block's Annual Report on Form 10-K filed with the SEC on February 23, 2021 (the “2020 10-K”), again detailed the material damage from a security breach by stating that:

If our privacy and security measures or those of third party developers and vendors are inadequate or are breached, and, as a result, there is improper disclosure of or someone obtains unauthorized access to or exfiltrates funds or other sensitive information on our systems or our partners' systems ... *our reputation and business could be damaged.* If the sensitive information is lost or improperly accessed, misused, disclosed, destroyed, or altered or threatened to be improperly accessed, misused, disclosed, destroyed, or altered, *we could incur significant financial losses and costs and liability associated with remediation and the implementation of additional security measures and be subject to litigation, regulatory scrutiny, and investigations.*

2020 10-K at 26-27 (emphasis added).

22. The 2020 10-K reiterated that the Company was a prime target for hackers and other malicious actors, largely repeating the disclosure contained in the 2019 10-K.

23. On August 2, 2021, the Company filed with the SEC its Quarterly Report on Form 10-Q for the period that ended June 30, 2021 (the “2Q21 10-Q”), which was signed by Dorsey and Ahuja. The 2Q21 10-Q stated that: “Any errors, *data leaks*, *security breaches* or incidents, disruptions in services, or other performance problems with our products or services caused by external or internal actors could hurt our reputation and damage our customers’ businesses.” 2Q21 10-Q at 77.

24. On November 4, 2021, the Company filed with the SEC its Quarterly Report on Form 10-Q for the period ended September 30, 2021 (the “3Q21 10-Q”), which made substantially similar, if not identical, disclosures to those in the 2Q21 10-Q.

25. The November 4, 2021 3Q21 10-Q also stated that:

Additionally, if our own confidential business information were improperly disclosed, our business could be materially and adversely affected. A core aspect of our business is the reliability and security of our payments platforms. Any perceived or actual breach of security or other type of security incident, regardless of how it occurs or the extent or nature of the breach or incident, could have a significant impact on our reputation as a trusted brand, cause us to lose existing sellers or other customers, prevent us from obtaining new sellers and other customers, require us to expend significant funds to remedy problems caused by breaches and incidents and to implement measures in an effort to prevent further breaches and incidents, and expose us to legal risk and potential liability including those resulting from governmental or regulatory investigations, class action litigation, and costs associated with remediation, such as fraud monitoring and forensics. Any actual or perceived security breach or incident at a company providing services to us or our customers could have similar effects. Further, any actual or perceived security breach or incident with respect to the bitcoin and blockchain ledger, regardless of whether such breach directly affects our products and services, could have negative reputational effects and harm customer trust in us and our products and services.

3Q21 10-Q at 78.

**C. Block Violated Accepted Industry Cybersecurity Standards, Resulting in a Massive Undisclosed Data Breach**

26. Former employees are a known risk for causing data security breaches.<sup>6</sup> As a result, proper data security seeks to prevent former employees from gaining access to the PII maintained by companies on their data system and the failure to remove access and permissions from departing employee accounts is widely recognized as a major security blunder.<sup>7</sup> The Federal Trade Commission (“FTC”) similarly suggests that companies physically secure PII by “[l]imit[ing] access [to PII] to employees with a legitimate business need” and “[c]ontrol[ling] who has a key, and the number of keys” available to access PII.<sup>8</sup> The FTC has further cautioned that companies must “[r]estrict access to sensitive data.”<sup>9</sup> The FTC has concluded that a company’s failure to maintain reasonable and appropriate data security for consumer’s sensitive personal information is an “unfair practice” violating the FTC Act, 15 U.S.C. § 45. *See, e.g., FTC v. Wyndham Worldwide Corp.*, 799 F.3d 236 (3d Cir. 2015).

27. Breaches of security or hacks can be prevented by, for example, using an effective security information and event management (“SIEM”) system.<sup>10</sup> A SIEM system records events and activities on computer networks and looks for anomalous activities. Having encryption

---

<sup>6</sup> *See, e.g., Hacks Are Happening Because Ex-Employees Still Have Access*, Cyber Security Hub (Oct. 13, 2017), <https://www.cshub.com/executive-decisions/news/hacks-are-happening-because-ex-employees-still>.

<sup>7</sup> *See, e.g., Don’t Overlook Security When Offboarding Employees*, ID Agent (Mar. 25, 2022), <https://www.idagent.com/blog/dont-overlook-security-when-offboarding-employees/>.

<sup>8</sup> *Protecting Personal Information: A Guide for Business*, FTC (Oct. 2016), [https://www.ftc.gov/system/files/documents/plain-language/pdf-0136\\_proteting-personal-information.pdf](https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf), at 8.

<sup>9</sup> *Start With Security: A Guide for Business*, FTC (June 2015), <https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf>, at 3.

<sup>10</sup> *See, e.g., Hacks Are Happening Because Ex-Employees Still Have Access*, Cyber Security Hub (Oct. 13, 2017), <https://www.cshub.com/executive-decisions/news/hacks-are-happening-because-ex-employees-still>.

protocols in place and making data difficult to obtain, use, save, or disperse, can also foil attempts by ex-employees to access information improperly. *Id.*

28. After an employee leaves a company, any minimally effective security program requires that a company's information technology ("IT") department be promptly informed for password and login management, and to increase monitoring efforts to ensure credentials of a former employee are not being used or misused.<sup>11</sup> Best practice also includes periodically checking credentials and access because most users do not need access to sensitive data unless they're working on specific projects or need time-sensitive resources. *Id.*

29. As explained in an Osterman Research, Inc. white paper titled "What Decision Makers Can Do About Data Protection," faced with the growing number and variety of cyber threats, "'data protection' encompasses a range of offensive and defensive plays to ensure that data is used by the right person for the right task at the right time – and nothing else."<sup>12</sup> Osterman Research further explains that "[d]ata loss caused by malicious employees [is] less common than cases of inadvertent loss, but [is] frequently of greater negative impact to an organization" and generally falls into one of a few categories, including anger at being involuntarily terminated causing a desire for retaliation. *Id.* at 8.

30. Plaintiffs retained Monty Myers, who possesses an education, background, experience, training, and expertise, including information technology/security, developed over 45+ years, to conduct an analysis of the First Data Breach. He is the Founder and CEO of Eureka

---

<sup>11</sup> Douglas Bonderud, *Breaking Up, Breaking In? Sensitive Data and the Ex-Employee*, Security Intelligence (July 20, 2015), <https://securityintelligence.com/news/breaking-up-breaking-in-sensitive-data-and-the-ex-employee/>.

<sup>12</sup> Osterman Research White Paper, *What Decision Makers Can Do About Data Protection* (Aug. 2020), available at <https://www.vmware.com/content/dam/digitalmarketing/vmware/en/pdf/docs/vmwcb-whitepaper-what-decision-makers-can-do-about-data-protection.pdf>, at 1.

Software, actively engaged in handling and protecting the confidential and proprietary, and trade secret information of his company and its clients. For two decades, he has served as an expert witness for both plaintiffs and defendants in over 150 litigation matters. Mr. Myers states that, based upon his expertise and analysis of publicly available information, it is his “professional opinion that Block, Inc. and its subsidiary Cash App Investing LLC [] did not have adequate information security protections in place at least around the date of the December 10, 2021 data security breach [] as it relates to former employee and system access controls.” This opinion was further supported by his Bachelor of Science in Engineering from Texas A&M University and his substantial graduate level course work at the University of Texas and his IT security experience.

31. Despite the known risk of malicious activities by ex-employees and the practices described above to mitigate those risks, in or around December 2021, a former employee of Block (the “FE”) accessed the Company’s networks and downloaded certain reports of Cash App that the FE accessed as part of their past employment responsibilities. The FE downloaded PII for approximately 8.2 million Cash App Investing users (defined above as the “First Data Breach”), including names, Cash App brokerage account numbers, portfolio values, holdings, and certain trading activity, evidencing a lack of adequate security measures or controls over customer’s personal data provided to Block.

32. If minimally effective security programs had been in place, then the FE would not have been able to use their credentials to access Block’s network and download *any* information, let alone PII for approximately 8.2 million Cash App Investing users. In fact, the FE should not have had any access to PII for Block’s customers, even assuming the FE needed to maintain network access for some *bona fide* reason.

33. After markets closed on April 4, 2022, and nearly four months after the First Data Breach, Block filed a Form 8-K current report with the SEC disclosing the First Data Breach and stating:

On April 4, 2022, Block, Inc. (the “Company”) announced that it recently determined that a former employee downloaded certain reports of its subsidiary Cash App Investing LLC (“Cash App Investing”) on December 10, 2021 that contained some U.S. customer information. While this employee had regular access to these reports as part of their past job responsibilities, in this instance these reports were accessed without permission after their employment ended.

The information in the reports included full name and brokerage account number (this is the unique identification number associated with a customer’s stock activity on Cash App Investing), and for some customers also included brokerage portfolio value, brokerage portfolio holdings and/or stock trading activity for one trading day.

The reports did not include usernames or passwords, Social Security numbers, date of birth, payment card information, addresses, bank account information, or any other personally identifiable information. They also did not include any security code, access code, or password used to access Cash App accounts. Other Cash App products and features (other than stock activity) and customers outside of the United States were not impacted.

Upon discovery, the Company and its outside counsel launched an investigation with the help of a leading forensics firm. Cash App Investing is contacting approximately 8.2 million current and former customers to provide them with information about this incident and sharing resources with them to answer their questions. The Company is also notifying the applicable regulatory authorities and has notified law enforcement.

The Company takes the security of information belonging to its customers very seriously and continues to review and strengthen administrative and technical safeguards to protect the information of its customers. Future costs associated with this incident are difficult to predict. Although the Company has not yet completed its investigation of the incident, based on its preliminary assessment and on the information currently known, the Company does not currently believe the incident will have a material impact on its business, operations, or financial results.

34. As a result of this disclosure, the price of Common Stock, which had closed at \$145.19 per share on April 4, 2022, plummeted, closing at \$135.92, \$128.77, \$125.93, and \$123.22 per share on April 5, 6, 7, and 8, respectively. Similarly, as a result of the disclosure, the price of CDIs, which trade on the ASX and which had closed at AUD 191.44 per share on April 5, 2022, plummeted, closing at AUD 178.27, AUD 170.68, AUD 168.30, and AUD 164.48 per share on April 6, 7, 8 and 9, respectively.

35. Block has not publicly disclosed the reasons that the FE had access to sensitive information about its customers. Some experts believe that the breach came from an orphaned account still active on a third-party software as a service (“SaaS”) application like a cloud storage solution or from a lack of proper communication protocols between Block’s Human Resources and IT departments.<sup>13</sup> That FE’s access to proprietary information, if minimal effective protocols had been put in place, would have been revoked upon termination.<sup>14</sup> Block’s human resources department would have identified all current employees and its IT department would have been able to identify unauthorized activity by account on its network, particularly with respect to large downloads of sensitive customer PII.

---

<sup>13</sup> See Alicia Hope, *Over 8 Million Cash App Users Potentially Exposed in a Data Breach After a Former Employee Downloaded Customer Information*, CPO Magazine (Apr. 14, 2022), <https://www.cpomagazine.com/cyber-security/over-8-million-cash-app-users-potentially-exposed-in-a-data-breach-after-a-former-employee-downloaded-customer-information/>.

<sup>14</sup> See, e.g., *Firing an Employee? Don’t Forget About Removing Their Access*, IT Support Blog (Mar. 9, 2019), <https://insideoutnetworking.com/firing-an-employee-dont-forget-about-removing-their-access/>; *Employee Termination Checklist for IT*, Agio, <https://agio.com/employee-termination-checklist-for-it> (last accessed Apr. 12, 2024). Indeed, while Block’s SEC filings do not provide many details about human resources and information technology, its annual reports filed on Form 10-K, including the one repeatedly cited in the Scheme Booklet, state that its “[o]perating expenses [] include allocated overhead costs for ... human resources, and IT.”

**D. The Aftermath and Block’s Reaction to the Data Breach**

36. Block in its annual report on Form 10-K filed with the SEC on February 23, 2023 (“2022 10-K”), amended the language in the risk factor disclosures relating to the protecting of Private Information referenced above, acknowledging the materiality of the Data Breach, including costs investigation, response, and the likelihood of other liabilities, stating in relevant part that:

[I]f our ... data protection[] or information security measures ... are inadequate or are breached or otherwise compromised, and, as a result, there is improper disclosure of or someone obtains unauthorized access to or exfiltrates ... sensitive data on our systems ... our reputation and business could be damaged. If the sensitive data or assets are lost or improperly accessed, misused, disclosed, destroyed, or altered or threatened to be improperly accessed, misused, disclosed, destroyed, or altered, we could incur significant financial losses and costs and liability associated with remediation and the implementation of additional security measures and be subject to claims, litigation, regulatory scrutiny, and investigations. *For example, in April 2022 we announced that we determined that a former employee downloaded certain reports of our subsidiary Cash App Investing in December 2021 that contained some U.S. customer information without permission after the former employee’s employment ended, as disclosed in our Current Report on Form 8-K filed with the SEC on April 4, 2022. We have incurred costs related to our investigation and response to this incident, and we could incur other losses, costs, and liabilities in connection with such incident.*”

2022 10-K (emphasis added).

37. As Block stated, negative publicity and litigation quickly followed, including the filing of *Salinas et al. v. Block, Inc. et al.*, No. 22-cv-04823 (N.D. Cal. Aug. 23, 2022), and *Gordon v. Block, Inc. et al.*, No. 22-cv-06787 (N.D. Cal. Nov. 2, 2022) (together the “Consumer Class Action”). The Consumer Class Action plaintiffs filed a consolidated complaint in February 2024 alleging their accounts were hacked because of Block’s failure to protect their private data and timely notify them of the breach. *See* Consumer Consolidated Class Action Complaint, *Salinas et al. v. Block, Inc. et al.*, No. 22-cv-04823 (N.D. Cal. Feb. 9, 2024), ECF No. 72 ¶ 58.

38. The First Data Breach also proved not to be an isolated or random occurrence as Block disclosed a second large-scale data breach (the “Second Data Breach”) in June 2023. *Id.* ¶ 63. As noted in the Consumer Class Action, an undisclosed number of Cash App users nationwide received a letter alerting them of the Second Data Breach. The Consumer Class Action alleges how the Second Data Breach happened because Block and its Cash App subsidiary failed to take reasonable measures to protect the PII that they had collected, stored, and were responsible for protecting, even after the First Data Breach. *Id.* ¶ 122 (“Defendants’ willful failure to abide by these duties [regarding its customers PII] was wrongful, reckless and grossly negligent as a business practice.”).

39. The parties to the Consumer Class Action have subsequently provided notice that they have reached a proposed settlement agreement for \$15 million, which has not yet been preliminarily approved by the court. *See* Plaintiffs’ Amended Notice of Approval of Class Settlement, *Salinas et al. v. Block, Inc. et al.*, No. 22-cv-04823 (N.D. Cal. Apr. 8, 2024), ECF No. 87.

## **E. Materially False or Misleading Statements Made to Afterpay Shareholders**

### **1. Statements Regarding Block’s Internal Controls to Facilitate the Merger**

40. In August 2021, Block executives believed that they could obtain corporate synergies by merging Block and Afterpay. Block focuses on providing e-commerce services to small businesses and its Cash App offering lets consumers send money to one another via smartphone, purchase things with a prepaid debit card, and invest in bitcoin and slices of individual stocks. Because Afterpay provides buy now pay, later services that allow consumers to make payments for purchases in multiple instalments, Block’s executives concluded that Afterpay could help Block’s quest to become a financial technologies super app, which could expand access to consumers and drive additional revenue for sellers.

41. On or about August 2, 2021, after discussing potential collaborations since late 2020, Block and Afterpay entered into a Scheme Implementation Deed (as amended, the “Deed”) providing for Block to acquire all Afterpay ordinary shares (“Afterpay Shares”) in exchange for Block Securities pursuant to a court-approved scheme of arrangement (the “Scheme”) under Part 5.1 of Australia’s Corporations Act 2001 (Cth) (the “Corporations Act”). Holders of Afterpay Shares could elect to receive either (a) 0.375 shares of Common Stock (“New Common Stock”) or (b) 0.375 CDIs (“New Block CDIs”) representing ownership interest in shares of Common Stock issued by Block pursuant to a Deed Poll to be executed by Block and Block Sub in favor of all Afterpay shareholders (the “Deed Poll”), after which Afterpay would become a wholly owned subsidiary of Block Sub and an indirect wholly owned subsidiary of Block.

42. The Deed states that “[a]t the request of [Block] and [Block] Acquirer, Afterpay intends to propose the Scheme and issue the Scheme Booklet.” The Deed further explains that the Scheme Booklet would include “Information[,]” which was defined as “the information regarding [Block] (including in respect of the New [Block] Shares, New [Block] CDIs and the Merged Group) provided by [Block] to Afterpay in writing for inclusion in the Scheme Booklet, being information regarding [Block] required to be included in the Scheme Booklet under [the Corporations Act], Corporations Regulations or ASIC Regulatory Guide 60.”

43. In the Deed, Block represented and warrantied that “the [Block] Information provided in accordance with this document and included in, or incorporated by reference into, the Scheme Booklet ... as at the date of the Scheme Booklet ... will not contain any material statement which is misleading or deceptive nor contain any material omission having regard to applicable disclosure requirements and will comply in all material respects with the requirements of the

Corporations Act, the Listing Rules and all relevant regulatory guides and other guidelines and requirements of ASIC[.]” (Deed § 12.3(h)).

44. The Deed clarifies, in a section titled “further [Block] Information” that “[Block] must take all reasonable steps to assist Afterpay to implement the Scheme on a basis consistent with this document and as soon as reasonably practicable, and in particular must ... *promptly provide to Afterpay any further or new Information as may arise after the Scheme Booklet has been sent to Afterpay Shareholders and until the date of the [Special] Meeting as may be necessary to ensure that the Information contained in the Scheme Booklet is not, having regard to applicable disclosure requirements, false, misleading or deceptive in any material respect (including because of any material omission) and to ensure that there would be no breach of clause 12.3(h) [quoted in ¶ 43] if it applied as at the date on which the further or new [Block] Information arose[.]*” Deed § 5.3(e) (emphasis added).<sup>15</sup>

45. Section 10.16 of the Scheme Booklet advised Afterpay’s shareholders that Afterpay would update the Scheme Booklet if it became aware of, among other things, a material omission from the Scheme Booklet or a significant new matter than would have been required to be included to be in the Scheme Booklet if known about at the date of lodgment with ASIC.

46. The Scheme Booklet states that Block “publishes its privacy policies and terms of service, which describe its practices concerning the use, transmission, and disclosure of information.” The Scheme Booklet further states:

Square collects and uses a wide variety of information for various purposes in its business, including to help ensure the integrity of its

---

<sup>15</sup> Section 12.3 of the Deed contains Block’s representations and warranties, and §12.3(h) represents and warrants that the Square Information included or incorporated by reference into the Scheme Booklet or any amendment or supplement thereto “will not contain any material statement which is misleading or deceptive nor contain any material omission having regard to applicable disclosure requirements[.]”

services and to provide features and functionality to its customers. This aspect of Square's business, including the collection, use, disclosure, and protection of the information it acquires from its own services as well as from third-party sources, is subject to laws and regulations in the United States, the European Union, and elsewhere.

Accordingly, Square publishes its privacy policies and terms of service, which describe its practices concerning the use, transmission, and disclosure of information. As Square's business continues to expand in the United States and worldwide, and as laws and regulations continue to be passed and their interpretations continue to evolve in numerous jurisdictions, additional laws and regulations may become relevant to Square.

47. Block's "privacy policies and terms of service" referred to on page 80 of the Scheme Booklet, as of November 4, 2021, provided that:

**We have implemented technical and organizational measures designed to secure your personal information** from accidental destruction, loss, alteration and from unauthorized access, use, alteration, or disclosure. However, we cannot guarantee that unauthorized third parties will never be able to defeat those measures or use your personal information for improper purposes. You provide your personal information at your own risk.

48. Yet, despite acknowledging that Block's claimed data security measures against "actual or perceived data security incidents that Square or its service providers may suffer" were essential to protect against one of several "factors that could cause fluctuations in the market price of Square Class A Shares" (Scheme Booklet, p. 179), Block failed to disclose that Block, in fact, had not properly implemented "technical and organizational measures designed to secure [] personal information" and made no mention in the Scheme Booklet of the security flaws suffered at the time of either the Scheme Booklet or prior to Afterpay shareholders voting on the Transaction. In truth and in fact, because of the deficiency in the Company's data security measures, on December 10, 2022, Block suffered the First Data Breach.

49. On November 4, 2021, the Supreme Court of New South Wales approved of Afterpay distributing the Scheme Booklet and convening a special meeting (the “Special Meeting”) to obtain the necessary Afterpay shareholder approval of the Scheme.

50. Block exercised control over the contents of the Scheme Booklet relating to a discussion of Block’s business based upon the following:

(a) The Deed’s recitals acknowledge that “[a]t the request of [Block] and [Merger Sub], Afterpay intends to propose the Scheme and issue the Scheme Booklet.”

(b) The term “Regulator’s Draft” is defined to mean “the draft of the Scheme Booklet in a form acceptable to both parties which is provided to ASIC for approval pursuant to section 411(2) of the Corporations Act.”

(c) Afterpay was obliged to “consult with [Block] as to the content and presentation of ... the Scheme Booklet[.]”

(d) Section 5.6 of the Deed gives Block the ultimate authority over the form and content of the Block Information presented in the Scheme Booklet and the Cover of the Scheme Booklet confirms that “[Block] has provided and is responsible for the [Block] Information.”

(e) The Scheme Booklet states (on page 210) that “[Block] has given, and has not withdrawn before the date of this Scheme Booklet, its consent to be named in this Scheme Booklet in the form and context in which it is named and to the inclusion of the [Block] Information, on the basis set out in the ‘Responsibility for Information’ statement contained in the ‘Important Notices and Disclaimers’ included at the start of this Scheme Booklet.”

(f) The Scheme Booklet states (on page 224) that Block Information includes information therein regarding the Square Group, the Combined Group, the Scheme Consideration,

Block's intentions in relation to Afterpay, and specifically "includes the information contained in the Letter from Square's CEO and Chairman, questions 3, 4, 19–22, 25, 30–32, 49–53 of the Frequently Asked Questions and sections 3.1(b), 3.2, 3.4–3.6, 3.8, 3.10, the acknowledgement from Square in 3.11(b), 5, 6, 7.1, 7.3(a), 7.3(d), 7.3(g), 7.3(h), 7.4–7.6 and 9 (as it relates to US laws and Square's Certificate of Incorporation and Bylaws), but excludes the Afterpay Information, information provided by Afterpay to Square (or otherwise obtained from Afterpay's public filings on ASX and ASIC) contained in, or used for the preparation of, the information regarding the Combined Group and the Independent Expert's Report or the Independent Limited Assurance Report."

51. On or about November 5, 2021, the Scheme Booklet was mailed and emailed to Afterpay's shareholders and, *inter alia*, stated (on page CVii) that "[Block] has provided and is responsible for the [Block] Information" and Section 10.10 of the Scheme Booklet explains that Block had given, and not withdrawn, its consent to be named in the Scheme Booklet "in the form and context in which [it is] named"; "the inclusion of [its] respective reports or statements noted next to [its] name[] or the references to those reports or statements in the form and context in which they are included in this Scheme Booklet; and the inclusion of other statements in this Scheme Booklet which are based on or referable to other statements made by [it] in the form and context in which they are included[.]"

## **2. Defendant Dorsey's Involvement in the Afterpay Merger**

52. The Scheme Booklet prominently featured the following letter (on p. 9) from Dorsey to Afterpay's shareholders:

**Dear Afterpay Shareholder,**

The Square Board and management are excited to offer you the opportunity to participate in the combination of Square and

Afterpay, which will unite two companies aligned in a shared mission of economic empowerment and financial inclusion.

We built our business to make the financial system more fair, accessible, and inclusive, and Afterpay has built a trusted brand aligned with those principles. Together, we can better connect Square's largest ecosystems – Cash App and Seller– to deliver even more compelling products and services for merchants and consumers and ultimately better serve our customers around the world.

Square is recognised as an industry leader with customers across a diverse range of industries and countries. Businesses use Square to reach buyers online and in person, manage their business, and access financing. Individuals use Cash App to spend, send, store, and invest money. Square owns a majority ownership stake in TIDAL, a global music and entertainment platform that expands Square's purpose of economic empowerment to artists. We also recently launched TBD, a bitcoin focused open-developer platform with the goal of making it easier to create non- custodial, permissionless, and decentralized financial services.

As an Afterpay Shareholder, your vote is important in order to ensure the Scheme is implemented and you have the opportunity to participate in the future growth and performance of the Combined Group. On behalf of the Square Board, we look forward to welcoming you as a shareholder of Square, following the successful closing of this transaction.

Sincerely,

**Jack Dorsey**

President, Chief Executive Officer and Chairman of the Board

53. The Scheme Booklet in Section 5 included "Information on [Block]," including the following statements:

(a) Section 5.3[b][vii] stating that:

Square collects and uses a wide variety of information for various purposes in its business, including to help ensure the integrity of its services and to provide features and functionality to its customers. This aspect of Square's business, including the collection, use, disclosure, and protection of the information it

acquires from its own services as well as from third-party sources, is subject to laws and regulations in the United States, the European Union, and elsewhere.

(b) Section 5.21 (beginning at p.118) titled “Further Information,” stating that “[Block] files annual, quarterly and current reports, proxy statements and other information with the SEC. [Block]’s SEC filings are available to the public at the SEC’s website at [www.sec.gov](http://www.sec.gov) or at [Block]’s website....”

54. Section 7 of the Scheme Booklet addresses “Key Risks,” with Section 7.4 listing certain “Risks Associated with the Operations of the Combined Group” and stating, after four pages of small-print risks including that “Square’s business is subject to complex and evolving regulations and oversight related to privacy and data protection[,]” that:

The outline of risks in sections 7.4(g), (h), (i), and (j) is a summary only. More detailed information in relation to risk factors relating to the business and operations of [Block] can be found in [Block]’s Annual Report on Form 10-K for the year ended 31 December 2020, filed with the SEC on 23 February 2021, and [Block]’s Quarterly Report on Form 10-Q for the quarter ended 30 June 2021, filed with the SEC on 2 August 2021. [Block]’s SEC filings are available to the public at the SEC’s website at [www.sec.gov](http://www.sec.gov) or at [Block]’s website....

55. Block, in the 2020 10-K, identified the following risks factors, among others:

(a) Block’s “business depends on a strong and trusted brand, and any failure to maintain, protect, and enhance our brand would hurt our business” (emphasis removed) and explaining “[a]ny negative publicity about our industry or our company, ... our privacy, data protection, and information security practices, litigation, regulatory activity, ... and the experience of our customers with our products or services could adversely affect our reputation and the confidence in and use of our products and services. If we do not successfully maintain a strong and trusted brand, our business could be materially and adversely affected.”

2020 10-K at 20.

(b) “[Block], our sellers, our partners, and others who use our services obtain and process a large amount of sensitive data. Any real or perceived improper or unauthorized use of, disclosure of, or access to such data could harm our reputation as a trusted brand, as well as have a material and adverse effect on our business” (emphasis removed) and explaining “[i]f ... sensitive information is ... improperly accessed ... we could incur significant financial losses and costs and liability associated with remediation and the implementation of additional security measures and be subject to litigation, regulatory scrutiny, and investigations.” *Id.* at 26-27.

(c) “Our business is subject to complex and evolving regulations and oversight related to privacy and data protection” (emphasis removed) and explaining “[a]ny failure ... to comply with our privacy, data protection, or information security policies ... could cause our customers to reduce their use of our products and services, disrupt our supply chain or third party vendor or developer partnerships, and materially and adversely affect our business.” *Id.* at 39.

(d) “Our products and services may not function as intended due to errors in our software, hardware, and systems, product defects, or due to security breaches or human error in administering these systems, which could materially and adversely affect our business” (emphasis removed) including that “Our software, hardware, systems, and processes may contain undetected errors or vulnerabilities that could have a material adverse effect on our business, particularly to the extent such errors or vulnerabilities are not detected and remedied quickly. We have from time to time found defects in our customer-facing software and hardware, internal systems, and technical integrations with third-party systems, and new errors or vulnerabilities may be introduced in the future. If there are such errors or defects in our software, hardware, or systems, we may face negative publicity, government investigations, and litigation.... Any errors, data

leaks, security breaches, disruptions in services, or other performance problems with our products or services caused by external or internal actors could hurt our reputation and damage our customers' businesses.... Additionally, electronic payment, hardware, and software products and services, including ours, have been, and could continue to be in the future, specifically targeted and penetrated or disrupted by hackers and other malicious actors. Because the techniques used to obtain unauthorized access to data, products, and services and to disable, degrade, or sabotage them change frequently and may be difficult to detect or remediate for long periods of time, we and our customers may be unable to anticipate these techniques or implement adequate preventative measures to stop them. If we or our sellers or other customers are unable to anticipate or prevent these attacks, our sellers' or other customers may be harmed, our reputation could be damaged, and we could incur significant liability." *Id.* at 27-28.

56. The Scheme Booklet otherwise relied upon and directed Afterpay shareholders to the Company's SEC filings including in Section 5.8, which addresses Dorsey's employment agreement with Block and that of the Company's Chief Financial Officer, stating that "[f]urther information in relation to the remuneration of [Block]'s executive officers can be found in [Block]'s annual proxy statement, which is on file with the SEC" but continues by adding, in contrast to Section 5.21 and 7.24 of the Scheme Booklet, that "[Block]'s annual proxy statement is not incorporated into this Scheme Booklet."

57. The Scheme Booklet advised Afterpay shareholders that "[v]oting will take place at the online [Special] Meeting to be held at 10.00am on Monday, 6 December 2021," but that the meeting could be adjourned at that time.

58. On or about December 2, 2021, Afterpay announced to the Australian Securities Exchange Ltd ("ASX") that all regulatory conditions for the Scheme had been satisfied, other

than a condition precedent relating to Bank of Spain approval which was expected to be satisfied in mid-January 2022.

59. On or about December 6, 2021, the Special Meeting was opened and then adjourned to December 14, 2021.

60. In a December 7, 2021 court hearing, the Australian court approved the distribution of supplementary documents (the “Supplemental Information”) to holders of Afterpay Shares and an adjournment of the Court’s hearing to approve the Scheme. The Court’s December 14, 2021 opinion states, among other things, that Afterpay sought “the Court’s approval to dispatch supplementary disclosure materials to Afterpay shareholders in advance of the adjourned [Special] Meeting,” including information about the conditions of closing and why independent experts believe the share consideration was still fair after a decrease in Block’s share price.

61. On or about December 7, 2021, the Supplemental Information was disseminated to Afterpay shareholders, and no other information or “further [Block] Information” as defined by the Deed was sent to Afterpay’s shareholders following the disclosure of December 7, 2021.

62. The Supplemental Information, in part, included a second letter from Lonergan Edwards addressing the implications of a decrease in Square’s share price since the Scheme was announced, and indicating that Lonergan Edwards continued to view the scheme as fair and reasonable and in the best interests of Afterpay shareholders in the absence of a Superior Proposal. Lonergan Edwards stated that it believed the Scheme Consideration to be between A\$89 and A\$105, and the value of Afterpay Shares to be between A\$92 and A\$108 per share.

63. As noted above, on December 10, 2021, a former employee of Block (the “FE”) accessed the Company’s networks and downloaded certain reports of Cash App that FE

accessed as part of their past employment responsibilities. The FE downloaded PII for approximately 8.2 million Cash App Investing users, including names, Cash App brokerage account numbers, portfolio values, holdings, and certain trading activity, evidencing a lack of adequate security measures or controls over customer's personal data provided to Block.

64. Block failed to disclose to Afterpay shareholders or the investing public the facts relating to either the First Data Breach or Block's lack of internal controls.

65. On December 14, 2021, Afterpay reopened the Special Meeting and its shareholders approved the Scheme without knowing that the Company lacked adequate security measures or controls and that the First Data Breach had occurred on December 10, 2021.

66. On or about December 17, 2021, Afterpay issued an announcement with ASX disclosing that it had lodged orders made by the Supreme Court of New South Wales with the ASIC, and that as a result the Scheme was legally effective. Afterpay further disclosed that the Transaction was expected to occur in the first quarter of 2022 after approval by the Bank of Spain.

67. On or about December 17, 2021, the Australian court, without being informed of the Data Breach, held a hearing with respect to approval of the Scheme. The Australian court issued a decision on December 29, 2021, stating in relevant part that:

**Section 3(a)(10) of the Securities Act 1933 (US)**

[ ] As Mr Jackman had indicated at the first court hearing, Block will rely on the Court's approval of the scheme to qualify for an exemption from the registration requirements of the *Securities Act* 1933 (US) under § 3(a)(10) of that *Act*. The operation of that exemption has been noted in earlier case law including *Re Central Pacific Minerals NL* above at [28]-[34]; *Re Simeon Wines Ltd* (2002) 42 ACSR 454; [2002] SASC 204 at [21]-[26]; and *Re Solution 6 Holdings Ltd* above at [37]-[45], and, more recently, in *Re Boart Longyear Ltd* (No 2) (2017) 122 ACSR 437; [2017] NSWSC 1105 and *Re BoartLongyear Ltd* [2021] NSWSC 1269.

[] The orders I made at the second Court hearing included a notation that notice was given to this Court regarding Block's reliance on this exemption of a kind made in earlier cases. I also summarise several aspects of the schemes for this purpose, adopting Mr Jackman's summary of those matters:

- (a) The proposed amended scheme contemplates the issue of securities (being securities in Block (formerly Square) to be issued by Block) to Scheme Shareholders as consideration for their relevant Afterpay share;
- (b) Notice of the proposed reliance on the exemption was given to this Court prior to the commencement of the second Court hearing (see paragraphs 107 to 109 of the written submissions for the first Court hearing);
- (c) An independent expert report prepared by Messrs Edwards and Resende of Lonergan Edwards & Associates concludes that the amended scheme is in the best interests of scheme shareholders, which opinion was confirmed in their letter dated 6 December 2021 (Annexure A to the Shareholder Letter) and dispatched to Afterpay shareholders pursuant to the supplementary disclosure orders and released to the ASX on 7 December 2021;
- (d) The Court has held this hearing to consider the fairness and reasonableness of the amended scheme;
- (e) The second Court hearing was conducted in open court and any Afterpay shareholder subject to the amended scheme had standing to appear in opposition. Notice of the second Court hearing was given to Afterpay shareholders the subject of the amended scheme, and [by] an advertisement in the Australian newspaper on 9 December 2021; and
- (f) No Afterpay shareholder the subject of the amended scheme indicated an intention to appear to oppose the amended scheme or has opposed the approval of the amended scheme.

For these reasons, I made the orders sought by Afterpay at the conclusion of the second Court hearing in respect of the scheme.

68. On January 31, 2022, Block Sub completed its acquisition of all Afterpay Shares and Afterpay became an indirect wholly owned subsidiary of Block. In connection with the closing of the Transaction, Block issued 113,387,895 New Common Stock, including Common Stock underlying 95,377,954 New Block CDIs.

69. After markets closed on April 4, 2022, Block filed a Form 8-K with the SEC disclosing the First Data Breach, which occurred nearly four months before (on December 10, 2021), for the first time.

70. The price of Common Stock, in reaction to this disclosure, plummeted from its closing price of \$145.19 per share on April 4, 2022, to close at \$135.92, \$128.77, \$125.93, and \$123.22 per share on April 5, 6, 7, and 8, respectively. Similarly, the CDIs, which trade on the ASX, plummeted from AUD 191.44 per share on April 5, 2022, to close at AUD 178.27, AUD 170.68, AUD 168.30, and AUD 164.48 per share on April 6, 7, 8, and 9, respectively.

71. Despite this untimely subsequent disclosure, Sections 5 and 7 of the Scheme Booklet, and the information incorporated by reference therein, including the 2020 10-K, were materially misleading in suggesting that Block's data protection policies and procedures were effective while, at the same time, Block was failing to take basic security protections with respect to the PII of its customers, such as ensuring that former employees lacked access to the Company's networks and were unable to download the PII of Block's customers.

72. On February 28, 2024, OIP's counsel sent a Freedom of Information Act ("FOIA") request to the Consumer Financial Protection Bureau (the "CFPB") requesting:

a copy of all documents in the CFPB's possession pertaining to data security at Block, Inc. f/k/a Square, Inc. be produced for inspection in connection with claims being prosecuted against Block and certain of its directors and officers in the lawsuits captioned Official Intelligence Pty Ltd. v. Block, Inc. et al, Docket No. 1:23-cv-02789

(S.D.N.Y.), and *In re Block, Inc. Securities Litigation*, No. 22-cv-8636 (S.D.N.Y.). More specifically, this request seeks documents relating to any improper release of personal information by Block or its representatives. We are currently aware of two examples: (1) a former employee of Block accessing the Company's networks and downloading certain reports of Cash App on or about December 10, 2021, and (2) a subsequent data breach disclosed in or around June of 2023 pertaining to an undisclosed number of Cash App users nationwide.

73. On April 10, 2024, the CFPB denied that request as relating to an ongoing enforcement proceeding.

## V. CLASS ACTION ALLEGATIONS

74. Plaintiff OIP brings the claims asserted in Counts I and II of this action as a class action on behalf of persons and entities who acquired Block Shares in exchange for Afterpay securities pursuant to the Merger (the "Securities Act Class") and Plaintiffs Fotios Sotiropoulos, and Kevin Sawyer bring the claims asserted in Counts III through V on behalf of all persons who purchased or otherwise acquired Block securities during the period February 26, 2020, to April 4, 2022 (the "Exchange Act Class").

75. Excluded from the Securities Act Class and the Exchange Act Class (collectively the "Classes" and individually each "Class") are Defendants and their families, officers and directors of Defendants, affiliates of Defendants, at all relevant times, members of their immediate families and their legal representatives, heirs, successors or assigns and any entity in which defendants have or had a controlling interest.

76. The members of each Class are so numerous that joinder of all members is impracticable. While the exact number of Class members is unknown to Plaintiffs at this time and can only be ascertained through appropriate discovery, Plaintiffs believe that there are at least hundreds of members in each proposed Class based on, *inter alia*, the over 113 million Block Shares issued in the Merger and the number of issued Block shares before April 4, 2022. Record

owners and other members of the Class may be identified from records maintained by Block, Afterpay, or their transfer agents and may be notified of the pendency of this action by mail, using the form of notice similar to that customarily used in securities class actions.

77. Plaintiff Sotiropoulos's claims are typical of the claims of the members of the Exchange Act Class and Plaintiff OIP's claims are typical of the claims of the members of the Securities Act Class. All members of both Classes were similarly affected by Defendants' wrongful conduct in violation of federal law that is complained on behalf of that Class. Plaintiffs will fairly and adequately protect the interests of the members of the Classes. Plaintiffs have no conflicts with absent class members and have retained counsel competent and experienced in class and securities litigation.

78. Common questions of law and fact exist as to all members of each Class and predominate over any questions solely affecting individual members of each Class.

79. The following questions of law and fact are common to the Securities Act Class:

- (a) whether Block is liable pursuant to Section 12(a)(2) with respect to the Block Securities issued to former Afterpay shareholders in connection with the Transaction;
- (b) whether the statements made in the Scheme Booklet misrepresented or omitted to state material facts in connection with offering or soliciting the purchase of Block Securities;
- (c) whether Dorsey and McKelvey are control persons of Block within the meaning of Section 15 of the Securities Act; and
- (d) whether the members of the Securities Class are entitled to rescission or, alternatively, to the extent the Securities Class members no longer hold Block Securities, what is

the appropriate amount of money damages suffered arising from Defendants' violation of the Securities Act.

80. The following questions of law and fact are common to the Exchange Act Class:

(a) Whether the federal securities laws were violated by Defendants' acts as alleged herein;

(b) whether Defendants' alleged misconduct constituted a device, scheme, or artifice to defraud in violation of the federal securities laws as alleged herein;

(c) whether Defendants Dorsey, Ahuja, and McKelvey are control persons of Block within the meaning of Section 20(a) of the Exchange Act; and

(d) what is the appropriate amount of money damages suffered arising from Defendants' violation of the Exchange Act.

81. A class action is superior to all other available methods for the fair and efficient adjudication of this controversy since joinder of all members is impracticable. Furthermore, the harm suffered by individual Class members, who are geographically dispersed, may be relatively small, such that the expense and burden of individual litigation could make it impossible for members of the Class to individually redress the wrongs done to them. There will be no difficulty in the management of this action as a class action.

**FIRST CAUSE OF ACTION:  
(Brought by OIP, Only, for Violation of § 12(a)(2) of the Securities Act  
on Behalf of the Securities Act Class, Against Block and Dorsey)**

82. Plaintiff OIP repeats and realleges ¶¶ 1-81 by reference.

83. This Cause of Action is brought pursuant to §12(a)(2) of the Securities Act, 15 U.S.C. §77l(a)(2), on behalf of the Securities Act Class, against Defendants Block and Dorsey.

84. This Cause of Action does not sound in fraud and Plaintiff OIP is not alleging that Defendants acted with scienter or fraudulent intent, which are not elements of a § 12(a)(2) claim.

85. New Block CDIs and Block Stock are each a security within the meaning of the Securities Act and are not exempted from Section 12(a)(2). *See* 15 U.S.C §§ 77b(1), 77l(a)(2).

86. Block offered CDIs and Block Stock by means of the mails, through the Scheme Booklet, which is a prospectus as defined by the Securities Act. *See* 15 U.S.C § 77b(10) (defining a prospectus as a “prospectus, notice, circular, advertisement, letter, or communication, written or by radio or television, which offers any security for sale or confirms the sale of any security.”). There are two exceptions to the definition: (1) a document is not deemed a prospectus if it is proved that prior to or at the same time with such communication there was a written prospectus meeting certain statutory requirements of 15 U.S.C. § 77j and (2) a document is not deemed a prospectus if it states from whom a written prospectus meeting the requirements of 15 U.S.C. § 77j may be obtained and, in addition, does no more than identify the security, state the price thereof, state by whom orders will be executed, and contain such other information as the SEC may permit. Neither exception to that definition applies because there is no effective date of a registration statement and no communication identifying where a prospectus may be obtained. The Scheme Booklet, as supplemented, was mailings that included a letter and other information directly from Block at least confirming, if not explicitly offering, the sale of a security within the meaning of 15 U.S.C § 77b(3).

87. The Scheme Booklet, as supplemented, omits to state material facts necessary in order to make the Block Information, in the light of the circumstances under which they were made, not materially misleading, including the failure to maintain a system of internal control adequate to protect the personal data of Block’s customers, or that the First Data Breach had taken place.

88. By means of the defective Scheme Booklet, as supplemented, and the submissions made to the Supreme Court of New South Wales, Block and Dorsey promoted, solicited, and encouraged OIP and the Securities Act Class to vote in favor of the Scheme and thereby offered or sold the Block Securities issue to the Securities Act Class in connection with the Transaction.

89. The Prospectus omitted material facts, as alleged above. Defendants Block and Dorsey owed OIP and other members of the Securities Act Class the duty to make a reasonable and diligent investigation of the statements contained in the Scheme Booklet, as supplemented, to ensure that such statements were true and that there was no omission to state a material fact required to be stated to make the statements contained therein not materially misleading. Block and Dorsey, in the exercise of reasonable care, should have known of the materialization of risks contained in the Block Information in the Scheme Booklet.

90. OIP and the Securities Act Class did not know, nor in the exercise of reasonable diligence could OIP and the Securities Act Class have known, of the omissions contained in the Block Information in the Scheme Booklet at the time OIP and the Securities Act Class acquired Block Securities.

91. By reason of the conduct alleged herein, Block and Dorsey violated § 12(a)(2) of the Securities Act. As a direct and proximate result of such violations, OIP and the other members of the Securities Act Class who received Block Securities pursuant to the offer or solicitation conducted by Defendants names in this Cause of Action sustained damages in connection with their purchases of Block Securities. Accordingly, OIP and the other members of the Securities Act Class who hold the Block Securities issued pursuant to the Prospectus have the right to rescind and recover the consideration paid for their shares, and hereby tender their common stock to the Defendants sued herein or otherwise seek an equivalent measure of damages.

**SECOND CAUSE OF ACTION:  
(Brought by OIP, Only, for Violations of § 15(a) of the Securities Act  
on Behalf of the Securities Act Class, Against Dorsey and McKelvey)**

92. Plaintiff OIP repeats and realleges ¶¶ 1-91 by reference.

93. This Cause of Action is brought pursuant to §15 of the Securities Act, 15 U.S.C. §77l(a)(2), on behalf of the Securities Act Class, against Defendants Dorsey and McKelvey.

94. Dorsey and McKelvey were each control persons of Block by virtue of their positions as directors and/or senior officers of the Company. Indeed, Dorsey and McKelvey are identified in Block's SEC filings as two of the Company's three non-independent directors (the other non-independent director having joined the Board in connection with the Company's recent acquisition of TIDAL), and Dorsey is its highest-ranking officer.

95. Dorsey and McKelvey each had the ability to influence the policies and management of Block by their voting and dispositive control over Block, and did so. On November 3, 2021, Block's shareholders overwhelmingly voted in favor of the issuance shares to Afterpay's shareholders in connection with the scheme, with 862,282,663 votes cast for the proposal and 746,647 votes cast against the proposal solicited through a special proxy statement. Dorsey and McKelvey control over 60% of the outstanding voting power of Block's equity classes. As a result, the issuance of Common Stock in the Scheme, which required a quorum of a majority of the voting power issued and outstanding and a majority of the voting power of the shares of Square common stock present, was impossible without their support.

96. Dorsey and McKelvey had a financial interest in Block acquiring Afterpay in order to increase the holding value and marketability of their investment. Defendants Dorsey and McKelvey were each critical to effecting the Scheme, based on their signing or authorization of the signing of the Deed, by voting as directors to acquire Afterpay, by voting their shares in favor

of the Block Proxy Statement, and by having otherwise directed through their authority the processes leading to execution of the Scheme.

## **VI. ADDITIONAL ALLEGATIONS FOR EXCHANGE ACT CLAIMS BY ALL EXCHANGE ACT CLASS MEMBERS**

97. The following allegations are applicable, for pleading purposes, only to claims under §§10(b) and 20(a) of the Exchange Act. These Exchange Act claims incorporate by reference the substantive allegations above. The Exchange Act claims also incorporate by reference the “Materially False or Misleading Statements Made to Afterpay Shareholders” in Section IV.E, *supra*, as false or misleading statements and the reasons why they were false as stated herein.

### **A. Additional Exchange Act Materially False or Misleading Statements Issued During the Class Period**

98. The Class Period for the Exchange Act Claims begins on February 26, 2020. On that day, Block filed its Form 10-K with the SEC for the period ended on December 31, 2019. The 10-K emphasized the risk of a data breach and the potential material impact on Block’s business, but it failed to disclose that Block lacked adequate security measures or protection procedures to prevent a serious data breach.

If our privacy and security measures or those of third party developers and vendors are inadequate or are breached, and, as a result, there is improper disclosure of or someone obtains unauthorized access to or exfiltrates funds or sensitive information on our systems or our partners’ systems, or if we suffer a ransomware or advanced persistent threat attack, or if any of the foregoing is reported or perceived to have occurred, our reputation and business could be damaged. If the sensitive information is lost or improperly accessed, misused, disclosed, destroyed, or altered or threatened to be improperly accessed, misused, disclosed, destroyed, or altered, we could incur significant financial losses and costs and liability associated with remediation and the implementation of additional security measures and be subject to litigation, regulatory scrutiny, and investigations.

2019 Form 10-K at 19.

99. This 10-K further acknowledged Block’s managements heightened knowledge of the risk of inadequate security measures stating that “electronic payment products and services, including ours, have been, and could continue to be in the future, specifically targeted and penetrated or disrupted by hackers,” posing a material risk to Block and its core operations because “If we or our sellers or other customers are unable to anticipate or prevent these attacks, our sellers’ or other customers’ businesses may be harmed, our reputation could be damaged, and we could incur significant liability.” *Id.*

100. Similarly, Block’s Annual Report on Form 10-K filed with the SEC on February 23, 2021 detailed the material damage from a security breach but it failed to disclose that Block lacked adequate security measures or data protection procedures to prevent a serious data breach, stating:

If our privacy and security measures or those of third party developers and vendors are inadequate or are breached, and, as a result, there is improper disclosure of or someone obtains unauthorized access to or exfiltrates funds or other sensitive information on our systems or our partners’ systems ... ***our reputation and business could be damaged.*** If the sensitive information is lost or improperly accessed, misused, disclosed, destroyed, or altered or threatened to be improperly accessed, misused, disclosed, destroyed, or altered, ***we could incur significant financial losses and costs and liability associated with remediation and the implementation of additional security measures and be subject to litigation, regulatory scrutiny, and investigations.***

2020 10-K at 26 (emphasis added).

101. This 10-K reiterated that Block was at significant risk from hackers and other malicious actors, but it again did not mention that Block lacked adequate security measures or controls.

102. On August 2, 2021, Block filed with the SEC its Quarterly Report on Form 10-Q for the period that ended June 30, 2021, which was signed by Dorsey and Ahuja, and stated that:

“Any errors, *data leaks, security breaches* or incidents, disruptions in services, or other performance problems with our products or services caused by external or internal actors could hurt our reputation and damage our customers’ businesses.” 2Q21 10-Q at 77 (emphasis added). This statement again failed to disclose that Block lacked adequate security measures or controls to prevent a serious data breach.

103. On November 4, 2021, Block filed with the SEC its Quarterly Report on Form 10-Q for the period ended September 30, 2021 that made similar disclosures to those from before, and again failed to disclose that Block lacked adequate security measures or controls to prevent a serious data breach, stating:

Additionally, if our own confidential business information were improperly disclosed, our business could be materially and adversely affected. A core aspect of our business is the reliability and security of our payments platforms. Any perceived or actual breach of security or other type of security incident, regardless of how it occurs or the extent or nature of the breach or incident, could have a significant impact on our reputation as a trusted brand, cause us to lose existing sellers or other customers, prevent us from obtaining new sellers and other customers, require us to expend significant funds to remedy problems caused by breaches and incidents and to implement measures in an effort to prevent further breaches and incidents, and expose us to legal risk and potential liability including those resulting from governmental or regulatory investigations, class action litigation, and costs associated with remediation, such as fraud monitoring and forensics. Any actual or perceived security breach or incident at a company providing services to us or our customers could have similar effects. Further, any actual or perceived security breach or incident with respect to the bitcoin and blockchain ledger, regardless of whether such breach directly affects our products and services, could have negative reputational effects and harm customer trust in us and our products and services.

3Q21 10-Q at 78.

104. On January 12, 2022, Block announced on its Square website that it received “ISO 27001 certification,” validating the strength and effectiveness of Square’s information security

management system (ISMS) and signifying Block's commitment to securing both company and customer data.

### **Square announces ISO 27001 certification**

JAN 12, 2022

Square is excited to announce we're ISO 27001 certified.

What is ISO 27001?

ISO 27001 is the most internationally recognized standard for information security management. As a management standard, ISO 27001 has comprehensive requirements for active executive leadership involvement across areas such as policy, process, records, ownership, risk management, resourcing, and communication.

How did we achieve this?

To become certified, Square's compliance was validated by a third-party audit firm who extensively reviewed our information security management system, demonstrating our ongoing and systematic approach to information security.

What does this mean for our Sellers and Partners? *Achieving this certification validates the strength and effectiveness of Square's information security management system (ISMS) and signifies our commitment to securing both company and customer data.*

Security has always been a top priority for Square and *this certification is a major milestone that showcases our ongoing commitment to protecting our systems, our sellers, and their customers.* With this certification, Square joins an elite class of global enterprise organizations with mature information security practices. For more information about Square's security, please visit [squareup.com/security](https://squareup.com/security).

You can find Square's ISO 27001 certificate [here](#).

105. The January 12, 2022 ISO 27001 announcement was issued almost a month after the hack of eight million customers' PII and picked up by the press and repeated. For instance, stock market website MasterScreener published an article that same day on its website, entitled,

“Block: Square announces ISO 27001 certification,” repeating the announcement in its entirety.<sup>16</sup>

And while the press release was issued to assure investors and customers of Block’s data security, there was no mention of the massive Data Breach that had occurred on December 10, 2021.

106. On January 31, 2022, Block issued a press release announcing “the successful completion of the Scheme of Arrangement under which Block has acquired all of the issued shares in Afterpay.” While the press release touted Defendants excitement over the Afterpay merger, the better products and services they will deliver, and making the financial system more fair and accessible to everyone, there was no mention of the massive Data Breach of approximately 8.2 million customers that had occurred on December 10, 2021. The press release stated in relevant part:

“We’re excited to welcome the Afterpay team to Block and are eager to get to work,” said Jack Dorsey, Block co-founder and CEO. ***“Together, we’ll deliver even better products and services for sellers and consumers while staying true to our shared purpose of making the financial system more fair and accessible to everyone.”***

The acquisition furthers Block’s strategic priorities for its existing Square and Cash App ecosystems. Together, Square and Afterpay intend to enable sellers of all sizes to offer ‘buy now, pay later’ (BNPL) at checkout, give Afterpay consumers the ability to manage their installment payments directly in Cash App, and give Cash App customers the ability to discover sellers and BNPL offers directly within the app.

Today, Square also launched its first integration with Afterpay, providing Afterpay’s BNPL functionality to sellers in the United States and Australia that use Square Online for e-commerce. This new omnichannel commerce tool can help sellers attract new shoppers and drive incremental revenue from day one. For more information on this announcement, read the press release here.

\* \* \*

---

<sup>16</sup> *Block: Square announces ISO 27001 certification*, MarketScreener (Jan. 12, 2022), <https://www.marketscreener.com/quote/stock/BLOCK-INC-24935553/news/Block-Square-announces-ISO-27001-certification-37531392/> (last visited Apr. 12, 2024).

“I’ve long admired Block’s purpose to make the financial system more accessible and inclusive. I’m honored and excited to bring my global experiences to the diverse expertise of this Board,” said Ms. Rothstein.

107. On January 31, 2022, Block also filed an 8-K with the SEC stating, among other things, that Block completed its merger with Afterpay, but omitted the massive Data Breach of approximately 8.2 million customers that had occurred on December 10, 2021:

On January 31, 2022 (Pacific Standard Time)/February 1, 2022 (Australian Eastern Daylight Time), Block completed its previously announced acquisition of all ordinary shares of Afterpay Limited, an Australian public company limited by shares and listed on the Australian Securities Exchange (“Afterpay” and such shares, “Afterpay Shares”), pursuant to a court-approved scheme of arrangement under Part 5.1 of Australia’s Corporations Act 2001 (Cth) (the “Scheme” and such acquisition, the “Transaction”), as contemplated by the Scheme Implementation Deed (the “Deed”), dated as of August 1, 2021 (Pacific Daylight Time)/August 2, 2021 (Australian Eastern Standard Time) (as amended by the Amending Deed, dated as of December 6, 2021 (Pacific Standard Time) / December 7, 2021 (Australian Eastern Daylight Time)), by and among Block, Afterpay and Lanai (AU) 2 Pty Ltd, an Australian proprietary company limited by shares and an indirect wholly owned subsidiary of Block (“Block Acquirer”).

Upon the implementation of the Scheme, all Afterpay Shares issued and outstanding as of 12:00 a.m. on January 21, 2022 (Pacific Standard Time) / 7:00 p.m. on January 21, 2022 (Australian Eastern Daylight Time), the record date for the Scheme, were transferred to Block Acquirer, and the holders of such Afterpay Shares (“Scheme Participants”) became entitled to receive, for each such share, either (a) where such Scheme Participant was a Share Elected Shareholder (as defined in the Deed), 0.375 shares of Block’s Class A common stock (“New Block Shares”); or (b) where such Scheme Participant was a CDI Elected Shareholder (as defined in the Deed), 0.375 CHESS Depositary Interests, each representing an ownership interest in a share of Block Class A common stock (“New Block CDIs”). In connection with the Transaction, 113,387,895 New Block Shares (including shares underlying 95,377,954 New Block CDIs) were issued to or for the benefit of Scheme Participants.

108. On February 24, 2022, Block published its annual Shareholder Letter, filed with the SEC on Form 8-K. While the Shareholder Letter documents detailed highlights from the fourth

quarter of 2021, and its successful efforts in acquiring new Cash App customers and driving their engagement, the letter omitted the fact that on December 10, 2021, a former employee downloaded reports containing sensitive PII on as many as 8.2 million customers, from Block's subsidiary, Cash App Investing. In relevant part the letter stated:

**To Our Shareholders**

We delivered strong growth at scale during the fourth quarter of 2021. Gross profit grew 47% year over year to \$1.18 billion, or 50% on a two-year compound annual growth rate (CAGR) basis. Our Cash App ecosystem delivered gross profit of \$518 million, an increase of 37% year over year and 90% on a two-year CAGR basis. For our Square (formerly known as Seller) ecosystem, gross profit was \$657 million, up 54% year over year and 32% on a two-year CAGR basis.

For the full year of 2021, gross profit was \$4.42 billion, up 62% year over year and 53% on a two-year CAGR basis. Cash App generated \$2.07 billion in gross profit, up 69% year over year and 113% on a two-year CAGR basis. Our Square ecosystem generated \$2.32 billion in gross profit, up 54% year over year and 29% on a two-year CAGR basis.

On January 31, we completed our acquisition of Afterpay, a global “buy now, pay later” (BNPL) platform. We believe this acquisition will further Block's strategic priorities for Square and Cash App by strengthening the connections between our ecosystems as we deliver compelling financial products and services for consumers and merchants. Together, we intend to enable Square sellers of all sizes to offer BNPL at checkout, offer Afterpay consumers the ability to manage their installment payments directly in Cash App, and give Cash App customers the ability to discover sellers and BNPL offers directly within the app. United by our shared purpose of economic empowerment, we are excited to welcome the Afterpay team to Block and help make the financial system more fair and inclusive as we build together.

**Cash App Ecosystem**

**Strengthening the network**

Peer-to-peer payments have allowed us to virally grow Cash App's network and remained the primary driver of customer acquisition in the fourth quarter. In December, there were more than 44 million

monthly transacting actives on Cash App, an increase of 22% year over year. To enhance network effects through other products, in the fourth quarter we introduced a new feature allowing customers to send fractional shares and bitcoin from their Cash App balances to friends and family. By expanding peer-to-peer capabilities, we see an opportunity to drive network effects across other products within our ecosystem and encourage customers to try new products within Cash App.

*In 2021, we also invested further in acquiring customers who value Cash App's ecosystem and engage with more products.* Behind these paid marketing investments, our acquisition cost in 2021 was approximately \$10 to acquire a new transacting active, and we've seen early monthly cohorts maintain strong returns on acquisition spend with paybacks of less than one year. Gross profit per monthly transacting active reached \$47 in the fourth quarter, an increase of 13% from the prior year, even as we grew our customer base.

#### **Driving engagement**

*As customers have adopted more products across Cash App, they have become more highly engaged and generated greater gross profit—particularly those who adopted Cash Card.* In December, there were more than 13 million actives who used Cash Card, representing 31% of our monthly active base. Customers have found broad-based utility with Cash Card through everyday purchases, and, as a result, spend per Cash Card active has increased over time. Cash Card is usually a customer's first banking product on Cash App and furthers adoption of products such as Boost or direct deposit. Cash Card has reached significant scale: In 2021, Cash Card gross profit was nearly half a billion dollars, up nearly 2x year over year as we both grew with existing customers and drove acquisition of new customers.

#### **Increasing inflows into our ecosystem**

Inflows into Cash App's ecosystem continued to be the primary driver of gross profit. Despite a roll off in government disbursements in the fourth quarter, we saw strength in recurring paycheck deposits, which we view as a key barometer of customers using Cash App for their primary banking needs. We also recently made improvements to the direct deposit customer experience by allowing customers to directly log in to their employer or payroll provider within the app, which provides another frictionless way for customers to get set up. *We remain focused on enhancing Cash*

***App’s financial services offerings to make it the banking platform of choice for customers[.]***

109. Also on February 24, 2022, Block issued the Company’s Annual Report on Form 10-K filed with the SEC on February 24, 2022 (the “2021 10-K”) signed by Defendants Dorsey and Ahuja.<sup>17</sup> In the 2021 10-K, the Company and the Individual Defendants again expressly emphasized the risk of a data breach, and the material impact on the Company that would be posed by such a breach. For example, it references “security breach(s)” at least ten times, “hack” seven times, and “stolen” customer data twice without once mentioning the Data Breach from December 10, 2021.

110. Under Risk Factors Summary/Operational Risks, in the 2021 10-K, the Company listed as potentially having a material impact on its business: (1) a real or perceived improper or unauthorized use of, disclosure of, or access to sensitive data; and (2) a real or perceived security breaches or incidents or human error in administering our software, hardware, and systems.

111. Under Operational Risks, in the 2021 10-K, Defendants repeated the risk to Block’s reputation and likelihood of a material and adverse effect on Block’s business should customer PII be breached:

We, our sellers, our partners, and others who use our services obtain and process a large amount of sensitive data. ***Any real or perceived improper or unauthorized use of, disclosure of, or access to such data could harm our reputation as a trusted brand, as well as have a material and adverse effect on our business.***

We, our sellers, and our partners, including third-party vendors and data centers that we use, obtain and process large amounts of sensitive data, including data related to our customers, our sellers’ customers, and their transactions. We face risks, including to our reputation as a trusted brand, in the handling and protection of this

---

<sup>17</sup> Defendant Dorsey certified, pursuant to SOX, that the 2021 10-K fully complied with the requirements of Section 13(a) or 15(d) of the Exchange Act and that the information contained in the 10-K fairly presented, in all material respects, the financial condition and results of operations of the Company.

data. These risks will increase as our business continues to expand to include new products, subsidiaries, and technologies, and as we and our third-party vendors rely on an increasingly distributed workforce. Our operations involve the storage and transmission of sensitive information of individuals and businesses using our services, including their names, addresses, social security/tax ID numbers (or foreign equivalents), government IDs, payment card numbers and expiration dates, bank account information, loans they have applied for or obtained, and data regarding the performance of our sellers' businesses.

\* \* \*

More generally, if our privacy, data protection, or data security measures or those of third party developers or vendors are inadequate or are breached or otherwise compromised, and, as a result, there is improper disclosure of or someone obtains unauthorized access to or exfiltrates funds, bitcoin, investment or other assets, or other sensitive information on our systems or our partners' systems, or if we, our third-party developers or vendors suffer a ransomware or advanced persistent threat attack, or if any of the foregoing is reported or perceived to have occurred, our reputation and business could be damaged. If the sensitive information or assets are lost or improperly accessed, misused, disclosed, destroyed, or altered or threatened to be improperly accessed, misused, disclosed, destroyed, or altered, we could incur significant financial losses and costs and liability associated with remediation and the implementation of additional security measures and be subject to claims, litigation, regulatory scrutiny, and investigations.

2021 10-K at 27-28.

112. The 2021 10-K again reflected that the Individual Defendants knew that the Company was an attractive target for hackers: “[E]lectronic payment[] ... products and services, including ours, have been, and could continue to be in the future, specifically targeted and penetrated or disrupted by hackers,” posing a material risk to Block and its core operations:

Because the techniques used to obtain unauthorized access to data, products, and services and to disable, degrade, or sabotage them change frequently and may be difficult to detect or remediate for long periods of time, we and our customers may be unable to anticipate these techniques or implement adequate preventative measures to stop them. *If we or our sellers or other customers are*

*unable to anticipate or prevent these attacks, our sellers' or other customers may be harmed, our reputation could be damaged, and we could incur significant liability.*

2012 10-K at 28.

113. These statements in the 2021 10-K were false and misleading as they failed to disclose the massive Data Breach of approximately 8.2 million customers that had occurred on December 10, 2021. The entirety of the 10-K was misleading.

114. The above statements identified were were also materially false and/or misleading, and failed to disclose material adverse facts about the Company's business, operations, and prospects. Specifically, Defendants failed to disclose to investors: (1) that the Company lacked adequate security measure, controls or protocols restricting access to customers' sensitive information; (2) that, as a result, a former employee was able to steal customer PII on as many as 8.2 million customers of the Company's subsidiary, Cash App Investing, containing full customer names and brokerage account numbers, as well as brokerage portfolio value, brokerage portfolio holdings and/or stock trading activity; (3) that, as a result, the Company was reasonably likely to suffer significant damage, including reputational harm and lawsuits; (4) and that, as a result of the foregoing, Defendant's positive statements above about the Company's business, operations, and prospects, and the Merger with Afterpay, were materially misleading.

**B. Scienter**

**1. Block and the Individual Defendants Were Long Aware of Red Flags Demonstrating Block's Derelict Data Security Practices**

115. Defendants were well aware of their vulnerabilities and inadequate security measures or controls over the protection of customer PII. *See* Section IV.C, *supra*.

116. In addition, ahead of the Merger Transaction, Cash App user accounts had been hacked on a number of occasions, resulting in fraudulent transfers of customer funds. In March

2021, it was reported that hackers accessed and took all the cash, stock, and bitcoin in certain Cash App customer accounts.<sup>18</sup> Cash App customers whose accounts had been hacked had attempted to contact Cash App about the incidents, but nothing was done. Many affected users found it nearly impossible to reach a live representative to discuss the security breaches. Scam artists played on affected users' frustrations by creating imposter company contact numbers to steal customers' account information. *Id.*

117. From February 2020 through March 2021, the Better Business Bureau (BBB) received and reviewed 2,485 complaints concerning Cash App and 3,532 concerning Square, where customers also logged Cash App complaints. In stark contrast, complaints for Venmo, a Cash App competitor, totaled a mere 928 and only 83 complaints were handled for Zelle. In 2020, before the Merger, Cash App user reviews mentioning the words "fraud" or "scam" had increased by 335%. *Id.*

118. An August 2021 *Medium* article discussed the proliferation of hacking attacks on Cash App and Block's lack of response. The Company's lack of internal controls was identified as the cause for the numerous security breaches: "A company, like Cash App, is however at fault for not having better blocks and ways to flag anything suspicious as well as having a dedicated way for customers to report fraud if it does happen."<sup>19</sup>

119. Facts also strongly infer that Defendant Dorsey was well aware of Block's deficient internal controls necessary to protect customer PII. Defendant Dorsey was a founder and the CEO

---

<sup>18</sup> See Alexis Keenan, *Square's Cash App vulnerable to hackers, customers claim: 'They're completely ghosting you,'* (Mar. 20, 2021), <https://finance.yahoo.com/news/squares-cash-app-vulnerable-to-hackers-customers-claim-113556593.html>.

<sup>19</sup> See Audrey Malone, *You Can Get Hacked on Cash App Easier than you Might Think*, Medium (Aug. 30, 2021), <https://medium.datadriveninvestor.com/you-can-get-hacked-on-cash-app-afbbf5420acf>.

of Twitter from May 2015 until November 29, 2021, and a director until May 22, 2022. In August 2022, a Twitter whistleblower complaint filed with three federal agencies—the SEC, the Department of Justice, and the FTC—was leaked to two major media outlets. The complainant, Peiter Zatko, was hired in 2020 by then-CEO Defendant Jack Dorsey to head cybersecurity in response to well-publicized breaches of celebrity and government official Twitter accounts.<sup>20</sup> Zatko claimed on July 6, 2022, that Twitter’s data security controls suffered from “egregious deficiencies, negligence and willful ignorance.”<sup>21</sup>

## **2. Defendants Are Presumed to Have Had Near Contemporaneous Knowledge of Security Breaches.**

120. Defendants are or should be presumed to have contemporaneous knowledge of their inadequate security measures or controls over the protection of customer PII, and more particularly the Data Breach. As described above, Defendants were well aware of the need to have strong protections of customer PII, aware of customer complaints, and government regulations and the need for best practices. *See* Section IV.A, *supra*.

---

<sup>20</sup> The 2020 hack was one of the most pronounced on a social media site and included the accounts of Joe Biden, Elon Musk, Jeff Bezos, Barack Obama, Microsoft co-founder Bill Gates, musician Kanye West, and both Uber and Apple also posted similar tweets, all instructing people to send cryptocurrency to the same bitcoin address. Rachel Lerman et al., *Biden, billionaires and corporate accounts targeted in Twitter hack*, The Washington Post (July 15, 2020), <https://www.washingtonpost.com/technology/2020/07/15/musk-gates-twitter-hack/>. In 2016 and 2019, Defendant Jack Dorsey’s account was hacked. Marie C. Baca, *Twitter co-founder Jack Dorsey’s account hacked*, The Washington Post (Aug. 30, 2019), <https://www.washingtonpost.com/technology/2019/08/30/twitter-founder-jack-dorseys-account-hacked/>. In 2016 and 2019 Defendant Jack Dorsey’s account was hacked. *Twitter co-founder Jack Dorsey’s account hacked*, The Washington Post (Aug. 30, 2019), <https://www.washingtonpost.com/technology/2019/08/30/twitter-founder-jack-dorseys-account-hacked/>.

<sup>21</sup> Whistleblower Disclosure of Peiter Zatko (July 6, 2022), available at [https://www.judiciary.senate.gov/imo/media/doc/Alpha%202.0%20Twitter%2020220706\\_Protected%20Whistleblower%20Disclosure\\_redacted\\_sanitized\\_opt.pdf](https://www.judiciary.senate.gov/imo/media/doc/Alpha%202.0%20Twitter%2020220706_Protected%20Whistleblower%20Disclosure_redacted_sanitized_opt.pdf).

121. Importantly, if in fact Block had adequate (or industry standard) systems in place, then they would have discovered the breach shortly thereafter. The ISO 27001 standard mandates prompt management reporting of security incidents and breaches. As such, it is reasonable to conclude that Block’s senior leadership knew or should have known about the breach within days of the discovery of its occurrence on December 10, 2021.<sup>22</sup>

122. Further supporting a strong inference that such a discovery was likely shortly after December 10, 2021, and known by the Defendants is the depth and particularity of Block’s admissions in their April 4, 2022 Form 8-K filing announcing it “recently determined that a former employee downloaded certain reports of its subsidiary Cash App Investing LLC (‘Cash App Investing’) on December 10, 2021,” and the fact that they were well into an investigation, had already been engaged with outside experts and were already notifying customers and regulators. There, the Company revealed that (1) the Company and its outside counsel had already launched an investigation with the help of a leading forensics firm, (2) that the company was already notifying customers, (3) that the Company already identified the perpetrator as a former employee who had regular access to these reports as part of their past job responsibilities, but in this instance these reports were accessed without permission *after their employment ended*, (4) that the Company could say with certainty what was taken, namely the “ full name and brokerage account number (this is the unique identification number associated with a customer’s stock activity on Cash App Investing), and for some customers also included brokerage portfolio value, brokerage portfolio holdings and/or stock trading activity for one trading day,” (5) and the Company could say what was not taken, namely “usernames or passwords, Social Security numbers, date of birth,

---

<sup>22</sup> [ISO 27001:2013 – Annex A.16: Information Security Incident Management | ISMS.online](#) and [ISO 27001 - Annex A.16 - Information Security Incident Management – ISO Templates and Documents Download \(iso-docs.com\)](#).

payment card information, addresses, bank account information, or any other personally identifiable information” nor “ any security code, access code, or password used to access Cash App accounts”, (6) that the Company knew already that no customers outside the US were impacted, and (7) that approximately 8.2 million current and former customers were already being notified and the Company was sharing resources with them to answer their questions as well as also notifying the applicable regulatory authorities and law enforcement.

123. These admissions of detailed knowledge strongly infer that the data breach came to the Defendants attention well before the announcement. Giving full credit to Defendants’ statements touting their ISO certification, which was actually obtained in November, 2021, it is more likely than not that the breach was discovered shortly after it occurred and even if the full details were not known, at a minimum, Defendants knew the severity and seriousness of it.

124. Plaintiffs retained an expert, Monty Meyers. Mr. Myers states that, based upon his expertise and analysis of publicly available information, it is his “professional opinion” that given his “understanding of the requirements/expectations on Block as a broker-dealer (e.g. SEC, FINRA, Sarbanes-Oxley, etc.), their status as an ISO 27001 certified company, and the technical/form nature of the data security breach, that [the December 10, 2021] breach would have been expected to be detected within days or weeks of its occurrence and is an indication of material inadequacies in Block’s access management, employee off-boarding, system monitoring, and data protection controls, particularly with respect to customer data.” Mr. Myers further states that these factors “also would lead me to conclude that more likely than not the breach was detected by the established data protection protocols/mechanisms at Block/CashApp within days or weeks of the breach, prior to Block’s January 12, 2022 press release regarding its ISO 270001 certification,

Block's February 24, 2022 10-K filing, and Block's April 4, 2022 8-K filing first disclosing the data security breach incident."

### **3. Motive**

125. Defendants had strong motives or incentives to keep the December 10, 2021 Data Breach and their inadequate and defective security measures and controls designed to protect customer PII hidden from investors.

126. The Block merger with Afterpay depended on Afterpay shareholder approval during a Special Meeting on December 14, 2021, an Australian court approving the Scheme on December 17, 2021, and the completion of the acquisition, which did not occur until January 31, 2022. Any acknowledgment by Block that its data security practices failed to meet industry standards before the Afterpay merger was complete would potentially undermine the planned merger and adversely impact Defendants' investment objectives by decreasing the holding value and marketability of their investments.

127. As a result, Defendants had both financial and reputational motives to conceal the December 10, 2021 Data Breach until April 4, 2022, when the Afterpay merger was fully completed and Defendants had consolidated their control of the acquired company.

### **4. Secrecy and Lack of Cooperation with Regulators**

128. Defendants' knowledge may also be inferred from Block's failure or refusal to publish the results of its investigation. At the time of the filing of this consolidated complaint—over three years after revealing the Data Breach—Defendants have not updated any information about the Data Breach, its cause, when and how they learned of the Data Breach, or its impact on customers' and Block's finances. For example, Block's SEC filings as recent as the 2023 10-K filed February 22, 2024, merely repeats "*in April 2022 we announced that we determined that a former employee downloaded certain reports of our subsidiary Cash App Investing in December*

*2021 that contained some U.S. customer information without permission after the former employee's employment ended, as disclosed in our Current Report on Form 8K filed with the SEC on April 4, 2022. We have incurred costs related to our investigation and response to this incident, and we could incur other losses, costs, and liabilities in connection with such incident."*

129. Similarly, Block has ghosted the CFPB. On October 21, 2021, the CFPB issued a series of orders, including one to Block (Square), to assist the CFPB monitor for data surveillance, access restrictions, and other consumer protection risks as payments technologies and markets evolve.<sup>23</sup>

The orders are issued pursuant to Section 1022(c)(4) of the Consumer Financial Protection Act. The CFPB has the statutory authority to order participants in the payments market to turn over information to help the Bureau monitor for risks to consumers and to publish aggregated findings that are in the public interest. The CFPB's work is one of many efforts within the Federal Reserve System to make payments safer, faster, and more competitive. The initial orders were sent to Amazon, Apple, Facebook, Google, PayPal, and Square.... Consumers expect certain assurances when dealing with companies that move their money. They expect to be protected from fraud and payments made in error, for their data and privacy to be protected and not shared without their consent, to have responsive customer service, and to be treated equally under relevant law. The orders seek to understand the robustness with which payment platforms prioritize consumer protection under laws such as the Electronic Fund Transfer Act and the Gramm-Leach-Bliley Act.

130. Some of the categories of information requested include identifying employee access to consumer PII, identified as "Direct or Indirect Product Data" in the order.

131. Similarly, in August 2022, the CFPB sued Block, accusing the company of "slow-walking" its responses to document demands the agency made in 2020 and 2021. On November

---

<sup>23</sup> *Order to File Information on Payments Products*, U.S. Consumer Financial Protection Bureau (Oct. 21, 2021), available at [https://files.consumerfinance.gov/f/documents/cfpb\\_section-1022\\_generic-order\\_2021-10.pdf](https://files.consumerfinance.gov/f/documents/cfpb_section-1022_generic-order_2021-10.pdf).

30, 2022, the district court ordered Block to comply by January 5, 2023. *See Consumer Financial Protection Bureau v. Block, Inc.*, No. 3:22-mc-80214-SK (N.D. Cal.).

132. Block's recent Annual Report on Form 10-K filed with the SEC on February 22, 2024 ("2022 10-K"), confirms there is an ongoing CFPB investigation. The 10-K states:

The Company received Civil Investigative Demands ("CIDs") from the Consumer Financial Protection Bureau ("CFPB"), as well as subpoenas from Attorneys General from multiple states, seeking the production of information related to, among other things, Cash App's handling of customer complaints and disputes. In December 2023, the CFPB notified the Company, pursuant to the CFPB's discretionary Notice and Opportunity to Respond and Advise ("NORA") process, that the CFPB's Office of Enforcement is considering recommending that the CFPB take legal action against the Company related to the topics addressed in its CIDs. The purpose of a NORA is to provide a party being investigated an opportunity to present its position to the CFPB before an enforcement action may be recommended or commenced. The Company is unable to predict the likely outcome of this matter and cannot provide any assurance that the CFPB will not ultimately take legal action against the Company or that the outcome of any such action, if brought, will not have a material adverse effect on the Company. The Company is cooperating with the CFPB and the state Attorneys General in connection with these inquiries.

2022 10-K at 146.

### **C. Loss Causation**

133. Defendants' false and/or misleading statements and omissions directly and proximately caused the economic loss suffered by Plaintiffs Sotiropoulos, Sawyer, and the Exchange Act Class. As a result of Defendants' materially false and misleading statements, omissions of fact, and fraudulent course of conduct, Block's securities traded at artificially inflated prices during the Class Period. Relying on the integrity of the market prices for Block securities and public information relating to Block, during the Class Period, Plaintiffs Sotiropoulos, Sawyer, and other Exchange Act Class members purchased or otherwise acquired Block securities at prices that incorporated and reflected Defendants' misrepresentations and omissions of material fact

alleged herein. The prices of Block securities significantly declined when the relevant truth concealed by Defendants' materially false and misleading statements and omissions, or the direct, proximate, and foreseeable effects thereof, were revealed, causing Plaintiffs Sotiropoulos, Sawyer, and other Exchange Act Class members to suffer losses. As a result of their purchases and acquisitions of Block securities during the Class Period at artificially inflated prices and the removal of that inflation upon the disclosures set forth in this Section, Plaintiffs Sotiropoulos, Sawyer, and the Exchange Act Class suffered economic losses (*i.e.*, damages) under the federal securities laws.

134. Plaintiffs Sotiropoulos and Sawyer and other Exchange Act Class members suffered actual economic loss and were damaged when the material facts and/or foreseeable risks concealed or obscured by Defendants' misrepresentations and omissions were partially revealed and or materialized through the disclosure of new information concerning Block on at least two dates: April 4, 2022, and March 23, 2023.

135. On April 4, 2022, Block announced that a former employee stole customer PII of its subsidiary Cash App Investing LLC ("Cash App Investing") on December 10, 2021, that contained some U.S. customer information, stating:

While this employee had regular access to these reports as part of their past job responsibilities, in this instance these reports were accessed without permission after their employment ended."

The information in the reports included full name and brokerage account number (this is the unique identification number associated with a customer's stock activity on Cash App Investing), and for some customers also included brokerage portfolio value, brokerage portfolio holdings and/or stock trading activity for one trading day....

Upon discovery, the Company and its outside counsel launched an investigation with the help of a leading forensics firm. Cash App Investing is contacting approximately 8.2 million current and former customers to provide them with information about this incident and

sharing resources with them to answer their questions. The Company is also notifying the applicable regulatory authorities and has notified law enforcement.

.... Future costs associated with this incident are difficult to predict. Although the Company has not yet completed its investigation of the incident, based on its preliminary assessment and on the information currently known, the Company does not currently believe the incident will have a material impact on its business, operations, or financial results.

136. On this news, the Company's common stock share price fell from \$145.19 (or \$9.27 or 6.4%) to close at \$135.92 per share on April 5, 2022. The price of Common Stock, plummeted, further closing at \$128.77, \$125.93, and \$123.22 per share on April 6, 7, and 8, respectively. Similarly, as a result of the disclosure, the price of CDIs, which trade on the ASX and which had closed at AUD 191.44 per share on April 5, 2022, plummeted, closing at AUD 178.27, AUD 170.68, AUD 168.30, and AUD 164.48 per share on April 6, 7, 8, and 9, respectively.

137. Plaintiffs Sotiropoulos, Sawyer and the Exchange Act Class may have experienced losses on other dates as Block's finances and/or ability to keep or grow customers and their engagement was impacted. Plaintiffs Sotiropoulos and Sawyer reserve the right to add those dates and the causation of the loss after discovery.

#### **D. Presumption of Reliance**

138. At all relevant times, the market for Block securities was an efficient market for the following reasons, among others:

(a) Block securities met the requirements for listing, and were listed and actively traded on NYSE, a highly efficient and automated market;

(b) As a regulated issuer, Block filed periodic public reports with the SEC and NYSE;

(c) Block regularly and publicly communicated with investors via established market communication mechanisms, including through regular disseminations of press releases on the national circuits of major newswire services and through other wide-ranging public disclosures such as communications with the financial press and other similar reporting services; and

(d) Block was followed by several securities analysts employed by major brokerage firm(s) who wrote reports which were distributed to the sales force and certain customers of their respective brokerage firm(s). Each of these reports was publicly available and entered the public marketplace.

139. As a result of the foregoing, the market for Block securities promptly digested current information regarding Block from all publicly available sources and reflected such information in the price of Block securities. Under these circumstances, all purchasers of Block securities during the Class Period suffered similar injury through their purchase of Block securities at artificially inflated prices and the presumption of reliance applies.

140. A class-wide presumption of reliance is also appropriate in this action under the Supreme Court's holding in *Affiliated Ute Citizens of Utah v. United States*, 406 U.S. 128 (1972), because the Exchange Act Class's claims are grounded on Defendants' failure to disclose and omission of material fact. Because this action involves Defendants' failure to disclose material adverse information regarding Block's business operations—information that Defendants were obligated to disclose—positive proof of reliance is not a prerequisite to recovery. All that is necessary is that the facts withheld be material in the sense that a reasonable investor might have considered them important in making investment decisions. Given the importance of the material adverse information alleged herein, that requirement is satisfied here.

**E. Inapplicability of Statutory Safe Harbor**

141. Block's "Safe Harbor" warnings accompanying ostensibly forward-looking statements issued during the Class Period were ineffective, are inapplicable to the fraudulent conduct alleged herein for the Exchange Act Class, and do not shield Defendants from any of the liability alleged herein.

**THIRD CAUSE OF ACTION:**

**(Brought by Sotiropoulos and Sawyer, Only, for Violation of § 10(b) of the Exchange Act and Rule 10b-5(a), (b) and (c) Thereunder on Behalf of the Exchange Act Class, Against All Defendants)**

142. Plaintiffs Sotiropoulos and Sawyer incorporate all of the foregoing by reference.

143. This Count is brought pursuant to §§10(b) of the Exchange Act, 15 U.S.C. §78j(b), and Rule 10b-5(a)(b) and (c) promulgated thereunder, on behalf of the Exchange Act Class, against all Defendants.

144. In connection with the purchase and sale of securities, Defendants knowingly or recklessly engaged in a device, scheme, artifice to defraud, act, practice, or course of business conduct that operated as a fraud and deceit upon Plaintiffs Sotiropoulos and Sawyer and the other members of the Exchange Act Class. Throughout the Class Period, the scheme: (i) deceived the investing public, including Plaintiffs Sotiropoulos and Sawyer and other Exchange Act Class members, as alleged herein; (ii) artificially inflated and maintained the market price of Block securities; and (iii) caused Plaintiffs Sotiropoulos and Sawyer and other members of the Exchange Act Class to purchase or otherwise acquire Block securities at artificially inflated prices. In furtherance of this unlawful scheme, plan and course of conduct, Defendants, and each of them, took the actions set forth herein.

145. Pursuant to the above device, scheme, artifice to defraud, act, practice, and courses of business conduct that Defendants employed and knew or recklessly disregarded would act as a fraud or deceit upon investors in Block securities, each Defendant participated in directly or

indirectly or were responsible for the device, scheme, artifice to defraud, act, practice, and course of business conduct that operated as a fraud or deceit on investors in Block securities.

146. Block, the Individual Defendants, and senior managers of Block and Afterpay whose scienter can be imputed and who are responsible for the device, scheme, artifice to defraud, act, practice, and course of business conduct had actual knowledge of the device, scheme, artifice to defraud, act, practice, and course of business conduct herein and intended thereby to deceive Plaintiffs Sotiropoulos and Sawyer and the other members of the Exchange Act Class, or, in the alternative, Defendants acted with reckless disregard of the device, scheme, artifice to defraud, act, practice, and course of business conduct in that they failed or refused to ascertain and disclose such facts as would reveal the device, scheme, artifice to defraud, act, practice, and course of business conduct and its impact on the price of Block securities. These acts and omissions of Defendants were committed willfully or with reckless disregard for the truth. Each Defendant knew or recklessly disregarded that material facts were being omitted as a direct result of the device, scheme, artifice to defraud, act, practice, and course of business conduct as described above.

147. Defendants are liable both directly and indirectly for the wrongs complained of herein. Because of their positions of control and authority, the Individual Defendants were able to and did, directly or indirectly, control the operations and content of the conduct of Block. As officers and directors of Block and Afterpay, the Individual Defendants had a duty to disseminate timely, accurate, and truthful information with respect to Block's businesses, operations, future financial condition, and future prospects. As a result of the device, scheme, and artifice to defraud alleged herein, the market price of Block securities was artificially inflated throughout the Class Period. As a result, Plaintiffs Sotiropoulos and Sawyer and the other members of the Exchange

Act Class purchased or otherwise acquired Block securities at artificially inflated prices and relied upon the price of the securities, the integrity of the market for the securities, and were damaged thereby.

148. During the Class Period, Block securities were traded on an active and efficient market. Plaintiffs Sotiropoulos and Sawyer and the other members of the Exchange Act Class, relying upon the integrity of the market, purchased or otherwise acquired Block securities at prices artificially inflated by Defendants' wrongful conduct. Had Plaintiffs Sotiropoulos and Sawyer and the other members of the Exchange Act Class known the truth, they would not have purchased or otherwise acquired Block securities or would not have purchased or otherwise acquired them at the inflated prices that were paid. At the time of the purchases or acquisitions by Plaintiffs Sotiropoulos and Sawyer and the Exchange Act Class, the true value of Block securities was substantially lower than the prices paid by Plaintiffs Sotiropoulos and Sawyer and the other members of the Exchange Act Class. The market price of Block securities declined sharply upon public disclosure of the facts alleged herein to the injury of Plaintiffs Sotiropoulos and Sawyer and Exchange Act Class members.

149. By reason of the conduct alleged herein, Defendants knowingly or recklessly, directly or indirectly, violated Section 10(b) of the Exchange Act and Rule 10b-5 (a) and (c) promulgated thereunder. As a direct and proximate result of Defendants' wrongful conduct, Plaintiffs Sotiropoulos and Sawyer and the other members of the Exchange Act Class suffered damages in connection with their respective purchases, acquisitions, and sales of the Company's securities during the Class Period.

**FOURTH CAUSE OF ACTION:  
(Brought by Sotiropoulos and Sawyer, Only, Violation of § 20(a) of the Exchange Act  
on Behalf of the Exchange Act Class, Against All Individual Defendants)**

150. Plaintiffs Sotiropoulos and Sawyer incorporate all of the foregoing by reference. This Count is brought pursuant to §20(a) of the Exchange Act, 15 U.S.C. § 78t(a), on behalf of the Exchange Act Class, against all Defendants.

151. The Individual Defendants were controlling persons of Block or Afterpay by virtue of, *inter alia*, their positions as the most senior officers and directors of Block and Afterpay, their substantial share holdings, their executive management positions, and their direct involvement in and responsibility for the negotiation, execution, and implementation of the Merger, and the device, scheme, and artifice to defraud alleged here, including the illicit sale of non-exempt, unregistered Block Shares alleged herein. The Individual Defendants had the power to exercise control over Block and Afterpay, and employees thereof, and exercised that power to control with respect to the Merger and the device, scheme, and artifice to defraud alleged here, including the illicit sale of non-exempt, unregistered Block Shares alleged herein. Each Individual Defendant also exercised control of Block, Afterpay, employees thereof, and the Merger through a series of direct or indirect business or personal relationships with other directors or officers or major shareholders of Block and Afterpay. Further, Block controlled its employees.

**PRAYER FOR RELIEF**

WHEREFORE, Plaintiffs pray for relief and judgment, as follows:

A. Certifying the Securities Act Class, appointing Plaintiff OIP as a class representative for the Securities Act Class and its counsel as Lead Counsel as Class Counsel for the Securities Act Class;

B. Certifying the Exchange Act Class and appointing Plaintiffs Sotiropoulos and Sawyer as class representatives for the Exchange Act Class and their counsel as Lead Counsel as Class Counsel for the Exchange Act Class;

C. Awarding compensatory damages in favor of Plaintiffs and the other Class members against all Defendants, jointly and severally, for all damages sustained as a result of Defendants' wrongdoing, in an amount to be proven at trial, including interest thereon;

D. Awarding rescission or a rescissory measure of damages to the Securities Act Class;

E. Awarding Plaintiffs and the Class their reasonable costs and expenses incurred in this action, including counsel fees and expert fees; and

F. Awarding such equitable/injunctive or other relief as the Court may deem just and proper.

#### **DEMAND FOR JURY TRIAL**

On behalf of themselves and all others similarly situated, Plaintiffs demand a trial by jury.

DATED: April 12, 2024

Respectfully Submitted,

By: /s/ Jeffrey S. Abraham  
Jeffrey S. Abraham  
Michael J. Klein  
**ABRAHAM, FRUCHTER & TWERSKY, LLP**  
450 Seventh Avenue, 38th Fl.  
New York, New York 10123  
Tel: (212) 279-5050  
Fax: (212) 279-3655  
jabraham@aftlaw.com  
mklein@aftlaw.com

*Co-Lead Counsel for Securities Act Claim Plaintiff*

Peretz Bronstein  
Yitzchak E. Soloveichik  
Eitan Kimelman  
**BRONSTEIN, GEWIRTZ & GROSSMAN, LLC**  
60 East 42nd Street, Suite 4600  
New York, NY 10165  
Tel: (212) 697-6484  
Fax: (212) 697-7296  
peretz@bgandg.com  
soloveichik@bgandg.com  
eitank@bgandg.com

*Co-Lead Counsel for Securities Act Claim Plaintiff*

By: /s/ Reed R. Kathrein  
Reed R. Kathrein (*pro hac vice*)  
Lucas E. Gilmore (*pro hac vice*)  
**HAGENS BERMAN SOBOL SHAPIRO LLP**  
715 Hearst Avenue, Suite 300  
Berkeley, CA 94710  
Telephone: (510) 725-3000  
Facsimile: (510) 725-3001  
reed@hbsslaw.com  
lucasg@hbsslaw.com

Nathaniel A. Tarnor  
**HAGENS BERMAN SOBOL SHAPIRO LLP**  
68 3rd Street, Suite 249  
Brooklyn, NY 11231  
Telephone: (212) 752-5455  
Facsimile: (917) 210-3980  
nathant@hbsslaw.com

*Lead Counsel for Exchange Act Claims Plaintiffs*

Brian J. Schall (*pro hac vice* forthcoming)  
**THE SCHALL LAW FIRM**  
2049 Century Park East, Suite 2460  
Los Angeles, CA 90067  
Telephone: (310) 301-3335  
Facsimile: (310) 388-0192  
brian@schallfirm.com

*Additional Counsel for Exchange Act Claims Plaintiffs*